

VYSOKÁ ŠKOLA BÁŇSKÁ – TECHNICKÁ UNIVERZITA OSTRAVA
EKONOMICKÁ FAKULTA
KATEDRA PRÁVA

Diplomová práce

Ochrana osobních údajů u vybraného podnikatele

Personal Data Protection of the Selected Entrepreneur

Student:

Bc. Martin Václavek, DiS.

Vedoucí diplomové práce:

Dr. Mgr. Michal Koziel, Ph. D.

Ostrava 2018

VŠB - Technická univerzita Ostrava
Ekonomická fakulta
Katedra práva

Zadání diplomové práce

Student: **Bc. Martin Václavek, DiS.**
Studijní program: N6208 Ekonomika a management
Studijní obor: 6208T011 Ekonomika a právo v podnikání
Téma: **Ochrana osobních údajů u vybraného podnikatele**
Personal Data Protection of the Selected Entrepreneur
Jazyk vypracování: čeština

Zásady pro vypracování:

1. Úvod
 2. Vymezení základních pojmů
 3. Povinnosti podnikatelů při ochraně osobních údajů
 4. Posouzení úrovně ochrany osobních údajů u vybraného podnikatele a návrhy pro futuro
 5. Závěr
- Seznam použité literatury
Seznam zkratk
Prohlášení o využití výsledků diplomové práce
Seznam příloh
Přílohy

Seznam doporučené odborné literatury:

BARTÍK, Václav a Eva JANEČKOVÁ. *Ochrana osobních údajů v aplikační praxi: vybrané otázky*. 4. aktualizované vydání. Praha: Wolters Kluwer, 2016. 287 s. ISBN 978-80-7552-141-5.
BĚLINA, Miroslav. *Zákoník práce: komentář*. 2. vyd. Praha: C. H. Beck, 2015. 1613 s. ISBN 978-80-7400-290-8.
KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*. Praha: Polygon, 2013. 167 s. ISBN 978-80-7273-173-2.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Dr Mgr. Michal Koziel, Ph.D.**

Datum zadání: 24.11.2017

Datum odevzdání: 27.04.2018

JUDr. Bohuslav Halfar
vedoucí katedry




prof. Dr. Ing. Zdeněk Zmeškal
děkan fakulty

Prohlášení

Já, níže podepsaný Bc. Martin Václavek, DiS., prohlašuji, a svým podpisem stvrzuji, že jsem diplomovou práci na téma Ochrana osobních údajů u vybraného podnikatele vypracoval zcela samostatně na základě literatury a pramenů uvedených v Seznamu použité literatury.

V Ostravě dne 26.4.2018


.....
Bc. Martin Václavek, DiS.

Poděkování

Z celého srdce bych rád poděkovala vedoucímu diplomové práce Dr. Mgr. Michalovi Kozielovi, Ph.D., za ochotu, poskytnuté materiály, zájem, připomínky a čas věnovaný vedení této diplomové práce.

Dále bych chtěl poděkovat celé mé rodině a přátelům, kteří mě podporovali po celou dobu mého studia a byli mi velkou oporou.

Abstract

The diploma thesis focuses on privacy and personal data protection in the employment sphere. The literature research part defines terminology necessary for understanding this issue, including the basic Czech legislation on the protection of privacy and private data. The original research part identifies processes of personal data and privacy protection in a specific factory. We have examined personal data processing from the moment of advertising a tender for a job position to cessation of employment, including monitoring employees during their employment. In the original research part there is a suggestion of what specific alterations the company should make to manage their employs data in accordance with the current Czech legislation.

Keywords

Personal data, sensitive data, privacy, proportionality principle, personal data administrator, data subject

Abstrakt

Diplomová práce se zaměřuje na ochranu soukromí a osobních údajů v pracovněprávních vztazích. V literární rešerši je definována terminologie nezbytná pro pochopení celé problematiky, včetně základní právní úpravy týkající se ochrany soukromí a osobních údajů v České republice. Vlastní práce identifikuje procesy ochrany osobních údajů a soukromí v konkrétní společnosti. Pozornost je věnována zpracovávání osobních údajů od chvíle vypsaní výběrového řízení, až po ukončení pracovního poměru, včetně monitoringu zaměstnanců při výkonu zaměstnání. Součástí vlastní práce jsou také návrhy doporučení pro zavedení konkrétních opatření ve společnosti tak, aby byla učiněna dostatečná náprava v souladu s právní úpravou České republiky.

Klíčová slova

Osobní údaj, citlivý údaj, soukromí, princip proporcionality, správce osobních údajů, subjekt údajů

Obsah

1	Úvod	10
TEORETICKÁ ČÁST.....		13
2	Vymezení základních pojmů	13
2.1	Soukromí.....	13
2.2	Ochrana osobnosti	13
2.3	Osobní údaj.....	14
2.3.1	Citlivý osobní údaj.....	15
2.3.2	Anonymní osobní údaj.....	16
2.3.3	Zveřejněný osobní údaj.....	16
2.3.4	Subjekt údajů	16
2.3.5	Správce a zpracovatel údajů	17
2.3.6	Příjemce údajů	17
2.3.7	Zpracovávání osobních údajů	18
2.3.8	Souhlas subjektu se zpracováním osobních údajů	18
2.3.9	Povinnosti správce a zpracovatele při zpracovávání osobních údajů	19
2.3.10	Práva subjektu údajů.....	19
2.4	Informace	20
2.5	Povinné subjekty.....	21
2.5.1	Veřejná správa	21
2.5.2	Státní správa.....	21
2.5.3	Samospráva.....	21
2.5.4	Subjekty veřejné správy.....	22
2.5.5	Veřejný zájem.....	22
2.6	Mezinárodní a evropská právní úprava ochrany osobních údajů	23
2.6.1	Všeobecná deklarace lidských práv a svobod.....	23

2.6.2	Evropská úmluva o ochraně lidských práv a svobod.....	23
2.6.3	Pravidla pro ochranu soukromí a přeshraniční toky osobních údajů.....	24
2.6.4	Úmluva 108	24
2.6.5	Směrnice 95/46/ES	25
2.6.6	Směrnice 2002/58/ES	25
2.7	Česká právní úprava ochrany osobních údajů	26
2.7.1	Listina základních lidských práv a svobod	26
2.7.2	Zákon o ochraně osobních údajů	27
2.7.3	Zákon občanský zákoník	28
2.7.4	Úřad pro ochranu osobních údajů.....	29
3	Základní povinnosti podnikatelů při ochraně osobních údajů	30
3.1	Hlavní znaky GDPR	31
3.2	Základní povinnosti spojené s GDPR.....	31
3.3	GDPR a zákon o ochraně osobních údajů	32
3.4	Základní povinnosti podnikatelů při ochraně osobních údajů	33
3.4.1	Shromažďování osobních údajů	34
3.4.2	Zpracování osobních údajů.....	34
3.4.3	Uchovávání osobních údajů.....	34
3.4.4	Blokování osobních údajů	34
3.4.5	Likvidace osobních údajů	35
3.4.6	Zveřejňování osobních údajů.....	35
3.4.7	Zpřístupnění osobních údajů.....	35
3.4.8	Anonymizace osobních údajů.....	35
PRAKTICKÁ ČÁST.....		36
4	Ochrana osobních údajů u vybraného podnikatele.....	36
4.1	Základní údaje společnosti	36
4.2	Zpracování osobních údajů společnosti XY	37

4.2.1	Zpracování osobních údajů před vznikem pracovního poměru.....	37
4.2.2	Zpracování osobních údajů v průběhu pracovního poměru.....	38
4.2.3	Zpracování osobních údajů po skončení pracovního poměru	39
4.3	Personální informační systémy	40
4.4.1	Lze cookies považovat za osobní údaje?	41
4.5	Příčiny zneužívání osobních údajů	42
4.6	Ochrana osobních údajů	43
4.6.1	Přístupová práva	43
4.6.2	Kryptování	43
4.6.7	Router	45
4.7	Archivace osobních dokumentů	45
4.8	Doporučení pro společnost	46
4.9	Aplikace GDPR pro společnost XY	47
4.9.1	Základní doporučení pro nadcházející účinnost GDPR:	49
5	Závěr	52
	Seznam použité literatury	54
	Prohlášení o využití výsledků diplomové práce.....	58
	Seznam použitých zkratk.....	59

1 Úvod

Právo na ochranu osobních údajů je jedno ze základních lidských práv každého člověka a to, jak ve veřejnoprávní, tak v soukromoprávní oblasti. Identifikace pomocí osobních údajů provází člověka po celou dobu jeho života, počínaje zápisem do matriky a přidělením rodného čísla či přihlášením k trvalému pobytu. Jsou zaznamenávány a uchovávány informace o našem zdravotním stavu, dosaženém vzdělání, spáchaných přestupcích či trestných činech atd. Osobní údaje a jejich používání jsou součástí běžného života člověka a jejich ochrana znamená ochranu jeho osobnosti.

Uchovávání osobních údajů a nakládání s nimi se stává čím dál diskutovanější, vzhledem k rostoucí globalizaci, využívání moderních technologií, internetu a dynamicky se rozvíjícímu světu. O osobní údaje se tak čím dál častěji nedělíme pouze pro nezbytně nutné účely, jako je založení bankovního účtu, smlouvy o pojištění nebo bankovního příp. hypotečního úvěru, ale dobrovolně je poskytujeme např. na internetu při registraci do internetového obchodu pro nákup běžného zboží, při vyplňování různých dotazníků, registracích do nejrůznějších soutěží nebo zakládání přístupu do sociálních sítí a jiných webových portálů.

Je-li tento trend rostoucí potřeby sdílení osobních údajů nevyhnutelný, měla by být také zajištěna ochrana těchto údajů, popřípadě zavedeny sankce za jejich zneužití. K tomu může dojít při nesprávném uchovávání osobních údajů a nakládání s nimi. Ty pak mohou být zneužity ve prospěch třetí osoby, což se postižený zpravidla dozví až od orgánů činných v trestném řízení, kdy se postižený neprávem ocitá v roli podezřelého. To může znamenat závažný zásah do lidských práv.

Každý člověk by měl znát práva, jež se týkají ochrany jeho osobnosti, tj. ochrany osobních údajů a zároveň každý, který jakýmkoli způsobem s osobními údaji nakládá, ať už jsou to lékaři, učitelé, policisté, podnikatelé aj., by měli vědět, jak s těmito údaji nakládat, aby nedošlo k jejich zneužití. Ochrana osobních údajů neznamena zákaz jejich používání, ale zabránění jejich zneužití, jelikož prakticky není možné se zpracovávání osobních údajů vyhnout.

Zpracovávání a uchovávání osobních údajů se týká každého z nás častěji, než si dokážeme představit a mnohdy ani netušíme, že jsme v postavení subjektu, s jehož osobními údaji je nakládáno a jaké jsou možnosti ochrany. Zároveň si mnozí podnikatelé neuvědomují, že i jich se týká povinnost ochrany osobních údajů, což s sebou přináší nepříjemný finanční

postih ze strany dozorových orgánů při nedodržení stanovených pravidel ochrany osobních údajů.

Velmi specifickému významu se dostává ochraně osobních údajů při jejich poskytování na internetu. Vědí poskytovatelé osobních údajů, jaká data smí subjekty, jenž osobní údaje shromažďují, získávat a jak by měly s tak citlivými daty nakládat? Dokážou tyto subjekty rozlišit, jaké povinnosti je nutno splnit vůči Úřadu na ochranu osobních údajů a jaká je souvislost mezi ochranou osobních údajů, jenž dozoruje inspektorát práce?

Ochrana osobních údajů je zakotvena v Deklaraci lidských práv, Evropské úmluvě o ochraně lidských práv a svobod, Pravidlech pro ochranu soukromí a přeshraničních toků osobních údajů, také v Úmluvě 108 a i Směrnice 95/46/ES se ochranou osobních údajů zabývá.

V ČR došlo k prosazení právní ochrany osobních údajů po roce 1989 se změnou společenského systému a připravovaným vstupem do EU. Pozornost této problematice začala být věnována až s rozvojem a rozšířením informačních technologií, kdy v roce 1992 byl vydán zákon číslo 256/1992 sb. o ochraně osobních údajů v informačních systémech. Postupem času byl zjištěn jako nedostačující, a bylo nutné vypracovat zákon nový.

Téma ochrany osobních údajů nabývá na důležitosti, jelikož díky vlivu Evropské unie nabude účinnosti nové evropské nařízení, tzv. GDPR. Jedná se o nařízení představující ucelený systém ochrany osobních údajů platící pro všechny členské země Evropské unie.

Diplomová práce je rozdělena do dvou kategorií, teoretická část vysvětluje všeobecné poznatky z oblasti ochrany osobních údajů, kdy jsou definovány základní pojmy, jako co to je osobní údaj, co je to citlivý osobní údaj, kdo je správcem osobních údajů a kdo je subjektem či příjemcem osobních údajů. Že existuje zpracovávání osobních údajů a že pro zpracování osobních údajů je potřeba určitého souhlasu. Dále se čtenář dovídá, jaké jsou povinnosti správce a zpracovatele se zpracováním osobních údajů, a naopak jaká jsou práva subjektů při zpracování osobních údajů. V teoretické části jsou také zveřejněny významné právní předpisy, které se ochrany osobních údajů dotýkají a také různé úmluvy a směrnice, na který se dotčený subjekt může obrátit v případě porušení ochrany osobních údajů. V třetí kapitole se čtenář může dočíst teoretické východiska nově platné a v budoucnosti účinné směrnice o ochraně osobních údajů, kterou přijal Evropský parlament. Nařízení GDPR přijde v účinnost dne 25. května 2018 a je potřeba se na ni připravit.

V praktické části diplomové práce jsou aplikována teoretická východiska a jsou zveřejněny základní informace o dané společnosti, a na základě analýzy u vybraného podnikatele jsou zveřejněny informace, jak daná společnost zpracovává osobní údaje, kde a

v jaké formě. Následně jsou zveřejněny i informace o využívání cookies a možné zpracování souhlasu s uchováváním osobních údajů. V závěrečné části praktické části jsou pak popsána doporučení. Vzhledem k blížící se účinnosti GDPR jsou zveřejněny jasné kroky, které by společnost měla v budoucnosti udělat, aby se dokázala na případnou účinnost daného nařízení kvalitně připravit.

Pro řešení daného zadání budou využity metody získávání vstupních údajů, deskripce, analýza, dělení a klasifikace. Nejčastěji bude využívána analýza a deskripce.

Cílem práce je zhodnotit stávající systém ochrany soukromí a osobních údajů v dané společnosti. Dále čtenáře, majitele společnosti a také malé a střední podnikatele seznámit s pojmem ochrana osobních údajů a pomoci jim udělat si pořádek v pojmech, které se týkají zpracování osobních údajů. Následně jim rozšířit informace o tom, které možné zákony, směrnice, a nařízení tuto problematiku řeší a v neposlední řadě jim přiblížit uvědomění si, že přichází v účinnost nové nařízení, které upravuje nově ochranu osobních údajů a tuto změnu je potřeba provést i v dané společnosti. Obsah práce by měl být návodem pro ty, kteří nemají jistotu v tom, jaké jsou požadavky kladené podnikatelům GDPR a jak konkrétně tyto požadavky ve své společnosti zavést.

TEORETICKÁ ČÁST

2 Vymezení základních pojmů

V následující kapitole budou vysvětleny základní pojmy, se kterými je spojena ochrana osobních údajů, jako například pojem soukromí, ochrana osobnosti, osobní údaj, definice citlivého osobního údaje, anonymního osobního údaje. Nesmí být opomenut úřad pro ochranu osobních údajů. Následně také vysvětlení pojmu veřejná správa, státní správa a samospráva se zaměřením se na informace o těchto subjektech a v neposlední řadě také objasnění pojmu veřejný zájem.

2.1 Soukromí

Soukromí může chápat každý jedinec svým způsobem. Nalézt přesnou definici tohoto pojmu je velmi složité. Někdo striktně odděluje soukromé od veřejného, naopak někdo do svého soukromí zahrnuje například práci, která představuje pro jiné věc veřejnou. Dle Občanského zákoníku (dále jen NOZ) v § 86 lze soukromí definovat jako nemožnost bez souhlasu určité osoby omezit prostory jemu vlastní, sledovat soukromý život či zaznamenávat audio či video záznam. Zároveň není možné pořízené záznamy otevřeně publikovat. Taktéž podléhají ochraně i písemné dokumenty.¹

Definice soukromí podléhá několika podmínkám, především místu a času, nelze také opomenout národnost, kulturní hodnoty a v neposlední řadě společenské postavení.²

Původní chápání soukromí bylo vymezováno jako specifický prostor, do kterého není možno, bez souhlasu dané osoby nebo na základě zákona, zasahovat.³

2.2 Ochrana osobnosti

Ochranou osobnosti se rozumí právo na ochranu základních lidských práv. Člověku by nemělo být upíráno žít dle svého nejlepšího vědomí a svědomí v kvalitním klimatu. V neposlední řadě je nutné dbát na ochranu lidské důstojnosti. Ochranou osobnosti se rozumí taktéž ochrana soukromí člověka.⁴

¹ Zákon č. 89/2012 Sb., § 86

² MORÁVEK, Jakub. Ochrana osobních údajů v pracovněprávních vztazích. Praha: Wolters Kluwer, 2013, s. 58. ISBN 978-80-7478-139-1

³ MATES, Pavel. Ochrana osobních údajů. Vyd. 1. Praha: Karolinum, 2002, s. 37. ISBN 80-246-0469-8

⁴ Zákon č.89/2012 Sb., § 81, odst. 1, odst. 2

Integrita člověka, tzv. nedotknutelnost je tvořena právem na život a zdraví.⁵

2.3 Osobní údaj

Již od pradávna existují znaky, které identifikují každou lidskou bytost, ovšem hovořit o jakési ochraně můžeme až v novodobé historii. V moderní společnosti byl významným milníkem holocaust, za něhož byly vytvořeny systémy evidující osobní údaje. Pro několik posledních desetiletí je typická masová distribuce lidských identifikátorů zvláště prostřednictvím internetu.⁶

Osobní údaj lze zpravidla charakterizovat jako základní charakteristiku osobnosti, lze zde zařadit například jméno, bydliště, kontakt na danou osobu, charakteristické vzhledové vlastnosti a podobně. Odborná literatura uvádí, že za osobní údaj lze považovat jakoukoliv informaci o člověku (fyzické osobě), kterou lze tuto osobu rozlišit od ostatních. Článek 4, Evropské unie obecné nařízení o ochraně osobních údajů nám definuje osobní údaj takto: „*Osobním údajem je jakákoliv informace týkající se určeného nebo určitelné fyzické osoby. Fyzická osoba se považuje za určenou nebo určitelnou, jestliže ji lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.*“⁷

Zákon o ochraně osobních údajů charakterizuje osobní údaj jako jakoukoliv informaci, která se týká určeného nebo určitelného subjektu údajů. Souhrn údajů a dat je považován za určený nebo určitelný, pokud lze subjekt údajů přímo či nepřímo charakterizovat, a to především na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.“⁸

Pojmy jako jsou určená nebo určitelná, lze v tomto smyslu vyložit jako soubor prvků, vlastností a dovedností, podle kterých lze přesně charakterizovat daného jedince, ke kterému se tyto prvky vážou. Zejména se jedná o číslo, kód či ostatní prvky, které jsou jedinečné pro fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.⁹

⁵ TELEČ, Ivo. Chráněné statky osobnostní, Právní rozhledy. 2007, roč. 15, č 8 s. 273. ISSN 1210- 6410

⁶ MATEŠ, P., E. JANEČKOVÁ a V. BARTÍK: Ochrana osobních údajů. Praha: Leges, 2012, 19 s. ISBN 978-80-87576-12-0

⁷ NOVÁ PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ: Měníme vize ve skutečnost [online]. Vydala Hospodářská komora České republiky, Odbor legislativy, práva a analýz, 2017, květen 2017, [cit. 2018-02-16]. Dostupné z: <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=4069>

⁸ ČESKO. § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-a>

⁹ MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana: knížka pro praxi. Vyd. 1. Praha: ASPI, 2003, 21-22 s. ISBN: 80-7357-322-9

Dle Kučerové a Nonnemanna lze osobní údaje dělit na identifikační, číselné, citlivé, audiovizuální a biometrické. Jméno, příjmení, adresa řadíme do skupiny identifikačních osobních údajů. Nezbytnou součástí života člověka jsou také číselné údaje, a to datum narození, rodné číslo, telefonní číslo, atd. Zdravotní stav, DNA, sexuální orientace, náboženské či politické smýšlení lze zaštitit pojmem citlivé údaje. Obrazové a zvukové záznamy, spolu s fotografiemi a snímky řadí mezi údaje audiovizuální. Další samostatnou skupinu tvoří biometrické údaje, kterými jsou otisky prstů, dlaně, částí těla či způsob chůze.¹⁰

2.3.1 Citlivý osobní údaj

Zvláštním druhem osobních údajů je citlivý osobní údaj, na který pamatuje také český právní řád a definuje tento údaj jako osobní údaj, který vypovídá o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu atd. Citlivý údaj můžeme také charakterizovat jako biometrický údaj umožňující přímou identifikaci nebo autentizaci subjektu údajů.¹¹

Kučerová a Nonnemann upozorňují, že se rodné číslo do taxativního výčtu citlivých údajů, podle § 4, písm. b) zákona o ochraně osobních údajů, neuvádí. Avšak z historického hlediska je rodné číslo velmi často využíváno, jedná se tedy o důležitý identifikátor a jeho ochrana je zaštitěna v § 13 písm. c) Zákona o evidenci obyvatel.¹²

Způsob, jak lze citlivé údaje zpracovávat je uveden v § 9 Zákona o ochraně osobních údajů.

O citlivých údajích se zmiňuje již Úmluva 108 a řadí je do kategorie „zvláštní skupina údajů“. Ve směrnici č. 95/46/ES je použit pojem „zvláštní kategorie údajů“. Na rozdíl od zákona směrnice zakazuje zpracování taxativním výčtem citlivých údajů, ale existují i jisté výjimky, např. nepřipouští zpracování údajů o původu, náboženském vyznání, sexuální orientaci, politické příslušnosti apod.

Podle § 9, písm. a) Zákona o ochraně osobních údajů je souhlas subjektu ke zpracovávání citlivých osobních údajů vyžadován písemně.

¹⁰ KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech, Praha, Vydavatel : RNDr. Ivana Hexnerová – BOVA POLYGON, 2013, 9 s., ISBN 978-80-7273-173-2

¹¹ČESKO. § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-b>

¹²KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech, Praha, Vydavatel : RNDr. Ivana Hexnerová – BOVA POLYGON, 2013, 11-12 s., ISBN 978-80-7273-173-2,

2.3.2 Anonymní osobní údaj

Pokud hovoříme o údajích, které nelze přiřadit žádné konkrétní osobě, pak se jedná o anonymní osobní údaje. Tudíž nelze tato data adresovat k určenému nebo určitelnému subjektu údajů, tzn. typickým znakem je neurčenost a neurčitelnost daného subjektu. Konkretizování subjektu je možno pouze při splnění určitých podmínek, což lze nazvat částečnou anonymizací.¹³

V případě, že zpracovatel nebo správce přiřadí tyto údaje ke konkrétní osobě, nadále se již nebude jednat o údaj anonymní.¹⁴

Dle § 5 odst. 1 písm. e) zákona, je nutno osobní údaje anonymizovat, a to v co nejkratší době, poté, co splnily svůj účel a jsou dále využívány v oblasti vědy, archivnictví či statistiky. Anonymizovat osobní údaje lze vyloučením některého z identifikátorů, např. jména, příjmení, místa narození. Aby byla anonymita účinná, nesmí existovat žádná možnost obnovy či opětovného přiřazení identifikačních znaků ke konkrétnímu subjektu.

2.3.3 Zveřejněný osobní údaj

Osobní údaj, který je poskytnut mediím nebo je šířen veřejnými sdělovacími prostředky, lze jej považovat za zveřejněný osobní údaj. Je-li osobní údaj součástí seznamu přístupného veřejnosti, také se hovoří o zveřejněných osobních údajích.

Osobní údaj, který lze dohledat na internetu, také spadá do kategorie zveřejněných osobních údajů.¹⁵

2.3.4 Subjekt údajů

Subjektem údajů musí být žijící fyzická osoba, která je právně způsobilá. Dle ZOOÚ není subjektem údajů právnická osoba.¹⁶

„Subjekt údajů představuje fyzická osoba, na kterou se osobní údaje vztahují.“¹⁷

¹³ MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. Osobní údaje a jejich ochrana. Knížka pro praxi. 1. vydání. Praha : ASPI, 2003, 34 s. ISBN: 80-7357-322-9

¹⁴ KUČEROVÁ, Alena. Zákon o ochraně osobních údajů: komentář. ISBN 978-807-1792-260.

¹⁵ SMEJKAL, V. a kol. Právo informačních a telekomunikačních systémů. 2. vydání. Praha: C.H.Beck, 2004, 161 s.

¹⁶ MORÁVEK, Jakub. Ochrana osobních údajů v pracovně právních vztazích. Praha: WoltersKluwer ČR, 2013, 200-201 s.

¹⁷ ČESKO. § 4 písm. d) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-d>

Dle Maštalky je subjekt údajů určená nebo určitelná fyzická osoba, jež je spojena s oněmi osobními údaji. Práva a zároveň také povinnosti získává dítě okamžikem narození a smrtí tato práva a povinnosti zanikají, čímž lze deklarovat vztah mezi subjektem údajů a živým člověkem.¹⁸

2.3.5 Správce a zpracovatel údajů

Správce dle ustanovení ZOOÚ § 4 písm. j) je každý subjekt, který udává účel a prostředky pro zpracování osobních údajů. Ten za ně zodpovídá a zpracovává je. *Zpracováním osobních údajů může správce zmocnit nebo pověřit zpracovatel, pokud zvláštní zákon nestanoví jinak.*¹⁹

Správce zpracovává osobní údaje sám, v případě, že zvláštní zákon nestanoví jinak, může tímto pověřit zpracovatele. Zpracovatelem podle zákona § 4 písm. k) je každý subjekt, který zpracovává osobní údaje na základě zákona nebo na základě pověření správcem. Může jimi být fyzická osoba, právnická osoba nebo stát jako vykonavatel veřejné moci, popř. některá jeho organizační složka.

Podle Matese, musí být správcem i zpracovatelem celý subjekt, který se zabývá technickým zpracováním a zabezpečením údajů.²⁰

2.3.6 Příjemce údajů

Příjemce je charakterizován jako jakýkoliv jednotlivec, kterému jsou sdělovány osobní údaje. Příjemce není charakterizován jako subjekt zpracovávající osobní informace za účelem inspekce, dohledu a regulace, která souvisí s výkonem veřejné moci²¹.

Jsou-li dané osobě osobní údaje odtajněny, lze ji nazvat příjemcem. Zatímco za příjemce nelze považovat zpracovatele osobních údajů podle § 3 odst. 6 písm. g.²²

¹⁸ MAŠTALKA, Jiří. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 33 s. ISBN 978- 80- 74-00-033-1

¹⁹ČESKO. § 4 písm. j) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-j>

²⁰ MATES, Pavel. Ochrana osobních údajů. Praha. Karolinum, 2002, 44 s. ISBN 80- 246-0469-8

²¹https://www.uoou.cz/files/ldv_prirucka_cz.pdf

²²ČESKO. § 4 písm. o) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-o>

Příjemcem může být osoba fyzická nebo právnická, orgán moci veřejné či jakákoli agentura, jíž jsou poskytovány údaje. Zatímco příjemcem není ten orgán, jenž získal osobní údaje při specifickém průzkumu.²³

2.3.7 Zpracovávání osobních údajů

Z hlediska právní úpravy ochrany osobních údajů je zpracování osobních údajů velmi podstatné. V ZOOÚ § 4 písm. e) se zpracovávání osobních údajů definuje jako „*jakákoliv operace nebo soustava operací prováděných správcem nebo zpracovatelem systematicky s osobními údaji, a to automaticky. "Zpracováním osobních údajů se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace.*“²⁴

Aby zpracování osobních údajů bylo legální, je podmínkou nabytí řádného právního titulu pro toto působení. Právní titul můžeme charakterizovat jako určitou licenci, která poskytuje oprávnění ke zpracování osobních údajů. Hackerská činnost je tedy nezákonná vzhledem k nezískanému a potřebnému právnímu titulu, což je v rozporu se zákonem 101/2000 Sb.²⁵

Vymezení tohoto pojmu je obsaženo i v dalších ustanoveních § 4 ZOOÚ. Uvedený výčet není taxativní, jelikož můžeme vzít v úvahu i jiné činnosti. Důležité je, aby správce či zpracovatel prováděl zpracování systematicky.²⁶

2.3.8 Souhlas subjektu se zpracováním osobních údajů

Maštalka pokládá souhlas se zpracováním osobních údajů za stěžejní a je upřednostňovaným právním důvodem pro nakládání s osobními údaji.²⁷

Souhlas ovšem není jediným titulem, na základě kterého je možné zpracovávat osobní údaje. Zpracování osobních údajů může být např. formou uzavření smlouvy o zpracování osobních údajů.

²³https://www.uouu.cz/files/ldv_prirucka_cz.pdf

²⁴ČESKO. § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-e>

²⁵ MAŠTALKA, Jiří. Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 46 s. ISBN 978- 80- 74-00-033-1

²⁶ MATES, Pavel. Ochrana osobních údajů. Praha. Karolinum, 2002, 44 s. ISBN 80- 246-0469-8

²⁷ MAŠTALKA, Jiří, Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 48 s. ISBN 978- 80- 74-00-033-1

Správce může zpracovávat osobní údaje pouze se souhlasem subjektu, ale občanský zákoník č. 89/2012 Sb. stanovuje v § 559 možnost libovolné formy v právním jednání, pokud není v rozporu se zákonem nebo ujednáním. Taktéž zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů nevyžaduje závaznou písemnou formu souhlasu subjektu. Ustanovení § 562 odst. 1 občanského zákoníku umožňuje provést písemný souhlas elektronický, popřípadě jinými technickými prostředky, taktéž přes internet. Tento souhlas však musí být zpětně prokazatelný.²⁸

Právem subjektu je vyslovit nesouhlas, který musí být vyjádřen písemně, v případě, že správce nebo zpracovatel osobních údajů hodlá tyto údaje dále využívat a není možno v případě nesouhlasu k daným osobním údajům připojovat další tyto údaje.²⁹

2.3.9 Povinnosti správce a zpracovatele při zpracovávání osobních údajů

Povinnosti správce a zpracovatele osobních údajů jsou upraveny v ZOOÚ v Hlavě II § 5 odst. 1. Než dojde ke zpracování osobních údajů, je potřeba stanovit účel zpracování osobních údajů, prostředky a způsob jejich zpracování. Jestli je účel obsažen v zákoně, není možná odchylka. Lze zpracovávat pouze údaje přesné a legálně získané a v případě potřeby data aktualizovat. Správce je oprávněn nepřesné údaje blokovat, opravit nebo doplnit, pokud se tak nestane, musí je zlikvidovat. Data lze uchovávat po dobu nezbytně nutnou nebo pro naplnění účelu.³⁰

Povinnosti správce jsou získaná data zabezpečit a chránit před vnitřním a vnějším zneužitím, popřípadě zneužití třetími osobami. Správce osobních údajů se musí řídit zákonem a přijmout opatření technická, organizační a právní.³¹

2.3.10 Práva subjektu údajů

Jedno ze základních práv subjektu je být informován o tom jak, budou jeho osobní údaje zpracovávány. Právo subjektu být informován, je v Zákoně o ochraně osobních údajů stanoveno hned několikrát.

²⁸<https://www.uoou.cz/lze-souhlas-se-zpracovanim-osobnich-udaju-ve-smyslu-5-odst-4-zakona-o-ochrane-osobnich-udaju-ucinit-i-elektronicky-mi-prostredky-napr-pres-internet/d-11336>

²⁹ KUČEROVÁ, Alena a František NONNEMANN. Ochrana osobních údajů v praktických příkladech, Praha, Vydavatel : RNDr. Ivana Hexnerová – BOVA POLYGON, 2013, 78 s., ISBN 978-80-7273-173-2

³⁰ČESKO. § 5 odst.1 zákona č. c),d),e),f) zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p5-1-c,d,e,f>

³¹ČESKO. § 13 odst.1,2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p13-1,2>

V § 5 odst. 4 ZOOÚ v případě, že subjekt udělil souhlas se zpracováním osobních údajů, má právo být informován o účelu zpracování, o jakého správce se jedná a o době uchování osobních údajů.

V § 11 odst. 1 má právo na informaci o rozsahu, účelu a konkrétním zpracování. Dále na informaci o právu k přístupu k osobním údajům a právu na opravu těchto údajů.

Dle § 5 odst. 6 písm. c) subjekt musí být informován, že jeho osobní údaje budou předány jinému správci. S tímto má právo nesouhlasit. Nesouhlas musí mít písemnou podobu.

2.4 Informace

Pojem informace je latinského původu, odvozeno ze slova „informare“, což v překladu znamená udávat tvar či podobu, formovat představu, něco zobrazovat či vytvářet pojem. Nad tímto výkladem se zamýšlí prof. Cejpek, který pojem informace chápe jako pojem velmi všeobecný, mající mnoho významů a provázející každodenní lidskou činnost. Tento pojem je velmi variabilní a nelze je vystihnout pouze jednou jedinou definicí. Dle prof. Cejpků lze hovořit o pojmu informace pouze v případě, je-li adresát člověk, jakožto živá bytost. Snaha o definování pojmu informace přicházela od mnoha autorů v různých oblastech lidské působnosti, avšak nepřinesla onen kýžený efekt. Laická veřejnost mnohdy nesprávně označuje informaci jako zprávu, sdělení, jakýsi přenos nebo komunikaci.³²

Maštálka charakterizuje informaci jako slovo významově podobné slovu údaj nebo data. Jedná se také o určitou realitu, která je popisována. Je-li objektem popisu fyzická osoba, lze konstatovat, že se jedná o osobní údaj. Data charakterizující určitý objekt mohou být nazývána informacemi.³³

Za informaci lze považovat *„jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního“*.³⁴ Tato definice je zakotvena přímo v zákoně číslo 106/1999 Sb. o svobodném přístupu k informacím. Záleží ovšem na tom, jaké oblasti se daná informace dotýká, neboť chápání pojmu informace může být rozdílné právě na základě odvětví.

³² CEJPEK, Jiří. Informace, komunikace a myšlení. Praha : Univerzita Karlova v Praze. Nakladatelství Karolinum, 2005. 233 s.

³³ MAŠTÁLKA, Jiří, Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 5 s. ISBN 978- 80- 74-00-033-1

³⁴ ČESKO. § 3 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106#p3-3>

2.5 Povinné subjekty

Mezi orgány, které jsou povinny poskytovat informace vztahující se k jejich činnosti, jsou především státní orgány, územní samosprávné celky a jejich orgány a veřejné instituce. Dále jsou povinnými subjekty ty orgány, kterým bylo zákonem svěřeno rozhodování o právech, právech chráněných zájmech, dále také o povinnostech fyzických nebo právnických osob v oblasti veřejné správy.³⁵

2.5.1 Veřejná správa

Veřejnou správou se rozumí správa věcí veřejných ve veřejném zájmu, která je určena její nezastupitelnou funkcí, jakožto určitého sociálního působení na veřejné otázky podmíněné veřejnou interakcí.³⁶

Veřejná správa je správní činnost související s poskytováním veřejných služeb, řízením veřejných záležitostí na místní i centrální úrovni a zajišťováním záležitostí ve veřejném zájmu. Kromě této správní činnosti bývají za veřejnou správu označovány též správní orgány, které ji vykonávají, tedy především úřady. Činnosti veřejné správy a správních orgánů jsou vázány právem. V současné době je veřejná správa rozdělena na dvě základní skupiny a to státní správu a samosprávu.³⁷

2.5.2 Státní správa

Je část veřejné správy, která se uskutečňuje jménem a v zájmu státu. Stát vykonává prostřednictvím orgánů a úřadů přímo či nepřímo prostřednictvím třetích osob správu na základě zákona delegovanou. Mezi přímý výkon státní správy lze zařadit činnost ministerstev u nepřímého výkonu státní správy přenášíme působnost na jiné orgány obcí a krajů.³⁸

2.5.3 Samospráva

Samospráva je způsob řízení určitého celku, kdy daný subjekt o alespoň některých svých záležitostech rozhoduje sám autonomním způsobem, tedy „spravuje se sám“. Výhodou

³⁵ČESKO. fragment #f1945949 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106#f1945949>

³⁶KADLEČKA, Stanislav a Filip RIGEL. *Výkon státní správy – kompetence, odpovědnost* [online]. 16. září 2009, 19 [cit. 2018-02-21]. Dostupné z: www.mvcr.cz/soubor/vykon-statni-spravy-kompetence-pdf.aspx

³⁷PRŮCHA, Petr. *Základy správního práva a veřejné správy, obecná část*. 2. přepr. a dopl. vyd. Brno: MU v Brně, 1994. 260 s. ISBN 80-210-0886-5.

³⁸HENDRYCH, D. a kol. *Právníký slovník*. 2. rozšířené vydání. Praha: C. H. Beck, 2003, 983 s. ISBN 80-7179-740-5

samosprávy je, že je blíže spravovanému subjektu než vnější a centrální řízení, a proto by měla být při zabezpečování lokálních či zájmově vymezených záležitostí efektivnější a levnější.

Samostatnost v tomto smyslu je chápána jako autonomní způsob řešení daných záležitostí, důležité je ovšem veřejný zájem a právní rámec, který je stanoven, stát může zasahovat do činností těchto samosprávných celků, vyžaduje – li to ochrana zákona.³⁹

2.5.4 Subjekty veřejné správy

Správce osobních údajů jsou osoby, které pracují s osobními údaji, odpovídají za ně a zpracovávají je. Jedná se o fyzickou osobu správce, nebo právnickou osobu veřejného či soukromého práva. V případě že správce nemůže vykonávat své povinnosti osobně, může zmocnit jinou fyzickou osobu nebo právnickou osobu, jako zpracovatele.

Zpracovatel je subjekt, který je schopen zpracovávat osobní údaje dle ZOOÚ, a to hlavně na základě zvláštního zákona.⁴⁰

Za zpracovatele teda můžeme označit kteroukoliv právnickou osobu nebo fyzickou osobu, nebo jakýkoliv státní orgán a veřejný subjekt.

2.5.5 Veřejný zájem

Obsah pojmu veřejný zájem určuje závaznou normu. Obecně je veřejný zájem charakterizován jako zájem, který odpovídá potřebám společnosti (celku). Pokud však chceme nalézt v praxi jednoznačně přijímané měřítko pro srovnání umožňující stanovení veřejného zájmu, je to velice obtížné.⁴¹

Na určitý daný problém mohou cílové skupiny pohlížet různě. Na základě odlišných názorů a postojů budou tyto skupiny mít odlišná řešení. Autor uvádí příklad stavby dálnice. Jedná se o veřejný zájem? Jelikož ke stavbě dálnice je třeba vyvlastnění pozemku soukromého vlastníka. Nebo se jedná o porušení soukromého práva na soukromé vlastnictví? Z pohledu vlastníka se bude jednat o zasahování do jeho vlastnických práv, kdežto řidiči na toto řešení budou pohlížet jako na veřejný zájem.⁴²

³⁹ HENDRYCH, D. a kol. Právnický slovník. 2. rozšířené vydání. Praha: C. H. Beck, 2003, 875 s. ISBN 80-7179-740-5

⁴⁰ Ustanovení § 4 písm. k) ZOOÚ

⁴¹ MAAYTOVÁ, A., F. OCHRANA a J. PAVEL. *Veřejné finance v teorii a praxi*. Praha: Grada Publishing, 2015. Expert (Grada). ISBN 978-80-247-5561-8.

⁴² MAAYTOVÁ, A., F. OCHRANA a J. PAVEL. *Veřejné finance v teorii a praxi*. Praha: Grada Publishing, 2015. Expert (Grada). ISBN 978-80-247-5561-8.

2.6 Mezinárodní a evropská právní úprava ochrany osobních údajů

Právní úprava ochrany osobních údajů vznikala v 70. letech 20. století. S vývojem informačních technologií roste riziko zneužití osobních údajů, a proto bylo třeba řešit tento problém.⁴³

Při zkoumání právních aspektů ochrany osobních údajů člověka je třeba respektovat, že osobní údaj je jeden z mnoha atributů charakterizujících člověka. Jako reakce na rozpolcenou evropskou společnost vzniká Organizace spojených národů (dále jen OSN), která si klade za cíl zachovat celosvětový mír, bezpečnost všem lidem a spolupráci mezi národy.⁴⁴

Parlamentní shromáždění Rada Evropy si nechalo vypracovat průzkum o dostatečnosti či nedostatečnosti ochrany soukromí, z něhož vyplynulo, že není poskytnuta ochrana v dostatečné míře.⁴⁵

Vzhledem k vzrůstajícímu toku osobních údajů mezi státy, bylo potřeba legislativně zaručit ochranu osobních údajů na všech úrovních, a to národní, evropské a mezinárodní.⁴⁶

2.6.1 Všeobecná deklarace lidských práv a svobod

Všeobecná deklarace lidských práva a svobod, je základní dokument, který obsahuje nejznámější katalog lidských práv, jenž byl ratifikován v den jeho vzniku, a to 16. prosince 1948. Tento dokument lze v dnešní době brát jako právní obyčej, neboť existuje již dlouhou dobu, a lidé mají všeobecné povědomí o tom, co v něm mohou nalézt. Obsahuje 30 kapitol, ve kterých lze nalézt mnoho okruhů, jako právo na život, právo na soukromí, které se dotýkají ochrany osobních údajů. V neposlední řadě za zmínku stojí článek 12, podle kterého by neměl být nikdo vystavován svévolnému zasahování do soukromí, do rodinného života, nebo korespondence. „Každý má právo na zákonnou ochranu proti takovým zásahům nebo útokům.“⁴⁷

2.6.2 Evropská úmluva o ochraně lidských práv a svobod

Evropská úmluva o ochraně lidských práv a svobod byla podepsána Radou Evropy v Římě 1950a v platnost vstoupila 3. září 1953. Jedná se o velmi důležitou úmluvu o lidských

⁴³ MATES, Pavel. Ochrana osobních údajů. Praha : Nakladatelství Karolinum. 2002. 37 s. ISBN 80-246-0469-8

⁴⁴(Charta Organizace spojených národů a Statut Mezinárodního soudního dvora. Praha: Informační centrum OSN, 1998,

⁴⁵Zákon ochrany osobních údajů, s. 25

⁴⁶Zákon ochrany osobních údajů, s. 26

⁴⁷ Všeobecná deklarace lidských práv, New York, 10. prosince 1948, článek 12

právech a svobodách. Obsahuje také možnost domáhat se ochrany těchto lidských práv a svobod. Důležitým článkem v Evropské úmluvě o ochraně lidských práv a svobod je zejména článek 8 odst. 1, který obsahuje právo na soukromí. Do soukromí lze zasáhnout dle článku 8 odst. 2 pouze v nezbytných případech, a to v souladu se zákonem.⁴⁸

S rozvojem technologie se Rada Evropy usnesla na tom, že národní úmluva neposkytuje dostatečnou ochranu jednotlivců a jejich soukromí. V důsledku stále se rozšiřujícímu přenosu informací mezi státy, bylo nutné se důsledněji zabývat ochranou osobních údajů na mezinárodní úrovni.⁴⁹

2.6.3 Pravidla pro ochranu soukromí a přeshraniční toky osobních údajů

Dalším významným krokem v ochraně osobních údajů je rok 1980, ve kterém byl přijat právně nezávazný dokument Pravidla pro ochranu soukromí a přeshraniční toky osobních údajů (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data), který vydala Organizace pro hospodářskou spolupráci a rozvoj (OECD), jež má povahu spíše doporučení. Obsahuje důležité principy ochrany osobních údajů např. princip omezení sběru osobních dat, princip specifikace účelu sběru osobních dat, jejichž důležitost je významná i v dnešní době.⁵⁰

2.6.4 Úmluva 108

Úmluva č. 108 o ochraně osob s ohledem na automatizované zpracování dat byla prvním mezinárodním právně závazným dokumentem, který se zabývá ochranou osobních údajů. V lednu 1981 byla přijata Radou Evropy a dne 9. července 2001 Českou republikou. Od 1. listopadu 2001, kdy byla zveřejněna v mezinárodní sbírce smluv, vešla v platnost.⁵¹

Z důvodu, že Úmluva je závazná pro členské státy, kterými byla přijata, je základním kamenem pro právní úpravu ochrany osobních údajů. Tento dokument formuluje základní pojmy a zásady ochrany osobních údajů. Mezi pojmy můžeme zařadit osobní údaj, automatizovaný soubor dat, automatizované zpracování a správce souborů údajů. Mezi zásady, které jsou v ní obsaženy, patří zásada legitimacy, jež stanovuje, jak získat a zpracovat osobní údaje v souladu se zákonem. Dále zásada účelovosti, ve které je dáno, že osobní údaje

⁴⁸<https://www.zakonyprolidi.cz/cs/1992-209>

⁴⁹ Zákon o ochraně osobních údajů, s. 25, s. 26

⁵⁰<http://www.oecd.org/sti/ieconomy/15589535.pdf>

⁵¹ Úmluva č. 108 byla podepsána dne 8. září 2001, ratifikována 9. července 2001 a zveřejněna ve Sbírce mezinárodních smluv pod č. 115/2001, dne 1. listopadu 2001.

musí být zpracovány k přesně stanoveným účelům. Zásada časovosti udává, že údaje mohou být uchovány po dobu potřebnou ke splnění účelu. Další zásadou je zásada přiměřenosti, kdy osobní údaje nesmí přesahovat daný účel. A v neposlední řadě zásada přesnosti stanovující přesnost údajů, které je nutné v případě potřeby aktualizovat.⁵²

Tento výčet zásad však není ovšem konečný, jelikož dále upravuje například zásadu bezpečnosti, zásadu práva na opravu a výmaz, zásadu přístupu k datům. Z hlediska závažnosti je potřeba zmínit čl. 6 Úmluvy 108, který se věnuje v české právní úpravě citlivým údajům.⁵³

2.6.5 Směrnice 95/46/ES

Směrnice 95/46/ES o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a volném a pohybu těchto údajů vychází z Úmluvy 108 a byla schválena Evropským parlamentem a Radou v říjnu 1995. Ustanovení této směrnice musí všechny členské státy EU transformovat do své národní právní úpravy a na dodržování přijatých předpisů bude dohlížet orgán dozoru. Týká se jak automatizovaného, tak neautomatizovaného zpracování osobních údajů a předávání těchto údajů do třetích zemí. V čl. 1 je zakotvena ochrana fyzických osob, jak je dáno v úvodních ustanoveních.⁵⁴

Je třeba zdůraznit, že směrnice 95/46/ES se nevztahuje na oblast veřejné bezpečnosti, obrany, bezpečnosti státu, činnosti státu v oblasti trestního práva, jak je uvedeno v čl. 3. Dále se směrnice neuplatní při zpracování „*prováděném fyzickou osobou pro výkon výlučně osobních či domácích činností*“.⁵⁵

Zvláštní pozornost věnuje tato směrnice kategorie citlivých údajů jako je rasový nebo etnický původu, politický postoj, náboženské, filozofické přesvědčení, odborová příslušnost a informace o zdravotním stavu či sexuální orientaci. V čl. 8 se stanovuje, že státy si individuálně vytýčí podmínky zpracování citlivých údajů za použití určitého identifikátoru.⁵⁶

2.6.6 Směrnice 2002/58/ES

Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v oblasti elektronické komunikace. Impulsem vzniku směrnice byla rychle se rozvíjející telekomunikační technologie. Ochrana osobních údajů a soukromí uživatele veřejně

⁵² Úmluva č. 108, čl. 5 – pís. a), b), c), d), e)

⁵³ Úmluva č. 108, čl. 6

⁵⁴ <http://www.eurlex.cz/dokument.aspx?celex=31995L0046>, čl. 1

⁵⁵ <http://www.eurlex.cz/dokument.aspx?celex=31995L0046>, čl. 3

⁵⁶ Úmluva č. 108, čl. 8

dostupných služeb elektronických komunikací musí být nezávislá na seskupení a uspořádání různých složek nezbytných pro poskytování služeb, a na rozdělování nezbytných činností a úkonů mezi těmito díly.⁵⁷

2.7 Česká právní úprava ochrany osobních údajů

V České republice byla ochrana osobních údajů začleněna do práva na soukromí a jeho ochranu. S vývojem informačních technologií však roste riziko zneužití osobních údajů, a proto bylo třeba řešit tento problém. Česká republika se touto problematikou začala zabývat v posledním desetiletí 20. století. „*Právo na soukromí je považováno za nejuniverzálnější a nejrozsáhlejší ze všech osobnostních práv, chráněných občanským právem.*“⁵⁸

V souladu s Evropskou úmluvou je vnímána ochrana soukromí a tok informací jako stěžejní i v tuzemské legislativě.⁵⁹

2.7.1 Listina základních lidských práv a svobod

Dne 16. 12. 1992 dochází k vyhlášení usnesení předsednictvem České národní rady, kdy Listina základních lidských práv a svobod jsou částí ústavního pořádku České republiky.⁶⁰

Tento dokument vychází z Úmluvy 108.⁶¹

Nejeden z pilířů této listiny je článek 7 odst. 1, ve kterém je popsána integrita člověka a jejího soukromí. Restriktci integrity umožňuje pouze zákon. Dále článek 10 odst. 1, který upozorňuje na zachování důstojnosti člověka, jeho cti, pověsti a dobrého jména. Odst. 2 obsahuje zásady ochrany soukromí rodinného života. Právo na ochranu před zneužíváním, publikací či shromažďováním osobních informací je zaneseno v odst. 3. Článek 17 svým obsahem zahrnuje práva jako je svobodné vyjádření slovem, i v písemné podobě bez ohledu na státní hranice. Cenzura je považována za zcela nepřijatelnou, jedinou výjimkou je zákonné omezení. Klade důraz na respektování práv druhých a ochranu státu. V neposlední řadě zahrnuje i lidskou mravnost a zdraví člověka.⁶²

⁵⁷<http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS>, odstavec 46

⁵⁸ 1 MATES, Pavel. Ochrana osobních údajů. Praha : Nakladatelství Karolinum. 2002. 37 s. ISBN 80-246-0469-8

⁵⁹ MAŠTALKA, Jiří, Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 5-6 s. ISBN 978-80-7400-033-1

⁶⁰<https://www.psp.cz/docs/laws/listina.html>

⁶¹ MAŠTALKA, J., Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 6 s. ISBN 978-80-7400-033-1

⁶²<https://www.psp.cz/docs/laws/listina.html>

2.7.2 Zákon o ochraně osobních údajů

Zákon číslo 101/2000 Sb., o ochraně osobních údajů (dále jen „Zákon“) je základní a velmi důležitý právní předpis, který upravuje ochranu osobních údajů v souladu s právem Evropské unie a mezinárodními smlouvami. Zákon stanovuje jasná pravidla, jak nakládat s osobními údaji, určuje základní práva a povinnosti a v případě porušení tohoto zákona, jasně stanovuje sankce. K novelizaci docházelo vícekrát, ale zásadní aktualizací prošel z důvodu vstupu České republiky do Evropské unie.

Ochrana osobních údajů byla před Zákonem ošetřena také v zákoně č. 256/1992 Sb., o ochraně osobních údajů v informačních systémech.

Osobní údaje, které jsou vymezeny Zákonem, podléhají zpracování státních orgánů, orgánů územní samosprávy či jiným orgánům moci veřejné, taktéž fyzickými a právnickými osobami. Tyto údaje mohou být zpracovávány, jak automatizovaně, tak i manuálně. Je-li správce sídlo mimo území České republiky, i přesto se na něj Zákon vztahuje. Provádí-li správce zpracování na území České republiky, ale jeho sídlo je mimo území Evropské unie, je povinen zmocnit zpracovatele.⁶³

Zákon se nevztahuje na osobní údaje, které jsou zpracovávány fyzickou osobou, a to pouze pro vlastní potřebu a zároveň na nahodilě shromažďované osobní údaje, kterou již dále zpracovávány nejsou. Toto nahodilé seskupování identifikátorů může mít za následek nepřesnosti nebo neúplnosti v datech a nevzniklo z iniciativy správce, ale pouze na základě volního impulsu či z aktivity třetí osoby nebo vlivem náhodné události.⁶⁴

V § 3 odst. 6 lze nalézt několik výjimek, které mají své opodstatnění z důvodu hájení zájmů bezpečnostních, vojenských či ryze ekonomických.

Dle Mateše, Janečkové, Bartíka⁶⁵ jsou principy právní úpravy v zákoně o ochraně osobních údajů charakterizovány 9 zásadami:

1. Zásada legitimacy zpracování říká, že osobní údaje musejí být nabyty a zpracovány v souladu se Zákonem.
2. Zásada nezbytnosti udává, že shromažďování identifikátorů je možno pouze při stanovení účelu.

⁶³<https://www.zakonyprolidi.cz/cs/2000-101#cast1> § 3 odst. 5

⁶⁴<https://www.zakonyprolidi.cz/cs/2000-101#cast1> § 3 odst. 3,4

⁶⁵ MATEŠ, P., E. JANEČKOVÁ a V. BARTÍK: Ochrana osobních údajů. Praha: Leges, 2012, 19 s.

3. Zásada časového omezení stanovuje nezbytně nutnou dobu, po kterou musejí být data zpracována a uchována.
4. Zásada proporcionality vymezuje přiměřenost osobních údajů požadovanému účelu.
5. Zásada transparentnosti promítá všechny aspekty zpracování osobních údajů daného subjektu.
6. Zásada bezpečnosti pamatuje na ochranu osobních údajů z hlediska personálního, technického a organizačního.
7. Zásada práva přístupu k datům pojednává o možnosti zisku informací o uložení osobních údajů ve formě, jenž je subjektu srozumitelná.
8. Zásada práva na opravu a výmaz zdůrazňuje, že v případě nepřesnosti, neaktuálnosti či chyby je nutno sjednat nápravu.
9. Zásada nezávislého dozoru ukládá funkci dozorových orgánů pověřených dohledem na dodržování zásad a právních norem ochrany osobních údajů.⁶⁶

Zákon o ochraně osobních údajů představuje obecnou rovinu ochrany osobních údajů v České republice, ale existuje celá řada speciálních právních úprav, jež se detailně zaměřuje na vybrané oblasti.⁶⁷

2.7.3 Zákon občanský zákoník

Zákon č. 89/2012 Sb. Zákon občanský zákoník (dále NOZ) je nejobecnějším právním předpisem upravujícím ochranu soukromí, jež je široce pojata. Vzhledem k původnímu zákonu č. 40/1964 Sb. a neustále se měnící ideové zaměření společnosti byla nutná několikerá novelizace. Nový občanský zákoník prošel mnohými změnami a jeho nové nasměrování lze považovat za správné.

Lidská důstojnost a svoboda člověka jsou předmětem § 3 odst. 1, zatímco odst. 2. stanovuje zásady charakterizující soukromé právo. Člověku nelze odeprít to, co mu přísluší, především právo na ochranu života, zdraví, svobody, úcty, důstojnosti a soukromí.

Ochrana jména, příjmení, rodného příjmení či dalších jmen člověka, také náleží do nového občanského zákoníku, a to do § 77 odst. 1.

⁶⁶ MATES, P., E. JANEČKOVÁ a V. BARTÍK. Ochrana osobních údajů. Praha: Leges, 2012, 9-26 s. ISBN 978-80-87576-12-0

⁶⁷ MAŠTALKA, Jiří, Osobní údaje, právo a my. 1. vydání. Praha: C. H. Beck, 2008, 154-159 s. ISBN 978-80-7400-033-1

Není možné bez svolení subjektu zachycení či šíření jeho podoby, ať už jako obrazový nebo zvukový záznam a není přípustné využívat pořízené záznamy třetí osobou, jak uvádí § 84 a § 85 NOZ.

Dle § 86 je zasahování do soukromého života ostatních nepřijatelné, není-li k tomu zákonný důvod. Stejně jako obrazové a zvukové záznamy, podléhají ochraně i záznamy písemné, nelze je využívat nepřiměřeně nebo poškozující zájmy člověka.

2.7.4 Úřad pro ochranu osobních údajů

Úřad pro ochranu osobních údajů je orgán, který je nezávislý a provádí dozor a dohled nad dodržování zákonem stanovených povinností při zpracování osobních údajů, vede registr povolených zpracování osobních údajů, dále přijímá podněty a stížnosti občanů na porušení zákona, a v neposlední řadě také poskytuje konzultace a hlavní informace v oblasti ochrany osobních údajů. Pro mnohé podnikatele může být základním stavebním kamenem při ochraně osobních údajů.

Činnost tohoto úřadu je vymezena zákonem číslo 101/2000Sb., ochraně osobních údajů a o změně některých zákonů a některými dalšími zákony. Tento zákon vznikl, aby ochraňoval občany státu a společně s Listinou základních práv a svobod zaručuje ochranu světa před neoprávněným, nelegálním zasahováním do soukromého života jedince, jedná se především o neoprávněné shromažďování, zveřejňování nebo jiné zneužívání osobních údajů. Vzhledem k tomu, že v dnešní době rozvoje informačních technologií, jsou tyto informace velice zneužívány, a proto přichází v platnost nové nařízení Evropského parlamentu a Evropské unie.

Úřad pro ochranu osobních údajů má velice pečlivě vypracovány osobní stránky (www.uoou.cz), kde si kterýkoliv občan české republiky může všechny veřejné rubriky pročit a také dovědět se mnoho informací, které jsou pro něj potřebné. Dále zde úřad zveřejňuje pravidelně své tiskové zprávy, názory úřadu na různé situace a dále jsou zde zveřejněny případy, které byly zveřejněny v médiích. Tato stránka by mohla být pro mnohé začínající podnikatele základním vodítkem, jak při svém podnikání neudělat chybu při ochraně osobních údajů.

3 Základní povinnosti podnikatelů při ochraně osobních údajů

Dne 25. května 2018 nahradí GDPR v českém právním řádu zákon č. 101/2000 Sb., o ochraně osobních údajů (dále „zákon o ochraně osobních údajů“ nebo „zákon“). Touto změnou začnou platit nová pravidla ochrany osobních údajů a to konkrétně vstoupí v účinnost nařízení Evropského parlamentu a Rady Evropské unie 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů) ze dne 27. 4. 2016, kterým se ruší směrnice 95/46/ES dále známá jako GDPR.

Obecné nařízení o ochraně osobních údajů (GDPR - General Data Protection Regulation) (EU) 2016/679 je nařízením EU o ochraně údajů a soukromí pro všechny jednotlivce v rámci Evropské unie. Zabývá se vývozem osobních údajů mimo EU. Cílem GDPR je především poskytnout občanům a obyvatelům kontrolu nad svými osobními údaji a zjednodušit regulační prostředí pro mezinárodní obchod sjednocením nařízení v rámci EU. Po zavedení GDPR nahradí směrnici o ochraně údajů z roku 1995 (směrnice 95/46 / ES). Byla přijata dne 27. dubna 2016. Stane se účinnou 25. května 2018 po dvouletém přechodném období. Na rozdíl od směrnice 95/46 / ES nevyžaduje, aby vnitrostátní vlády předkládaly jakoukoli legislativu, a proto jsou přímo závazné a použitelné.⁶⁸

GDPR usiluje o vytvoření harmonizovaného právního rámce v oblasti ochrany údajů v celé EU a jeho cílem je poskytnout občanům kontrolu nad jejich osobními údaji a současně uložit přísná pravidla týkající se hostingu a zpracování těchto údajů kdekoli ve světě. Nařízení rovněž zavádí pravidla týkající se volného pohybu osobních údajů v rámci EU i mimo ni.⁶⁹

Nařízení GDPR je velikým vodítkem pro mnoho podnikatelů, kteří mnohdy tápou v zákonných záležitostech týkajících se zveřejňování osobních údajů. Reaguje na technologický pokrok v oblasti informačních a komunikačních technologií, které se neustále vyvíjejí a zdokonalují. V rámci zpracování osobních údajů lze vidět z historického hlediska důležitý pokrok, neboť dnes se tyto informace zpracovávají komplexněji a používají se nové metody a způsoby uchovávání těchto dat. GDPR má za úkol posilovat ochranu dat občanů.

Nesmíme ovšem po přijetí GDPR úplně zapomenout na zákon o ochraně osobních údajů. Ten zde bude stále platný, ovšem dojde k omezení jeho rozsahu. V praxi jde tedy o to, že tento zákon se bude používat až v případě, kdy GDPR nebude něco upravovat, tudíž lze říci, že tento zákon se změní ze speciálního na pomocný.

⁶⁸ BLACKMER, W.S. 2016. „GDPR: Getting Ready for the New EU General Data Protection Regulation”. Information Law Group. Info Law Group LLP.

⁶⁹ <https://www.ibm.com/data-responsibility/gdpr/>

Nařízení Evropské Unie má přednost před zákonem. Je tzv. přímo aplikovatelné a závazné pro všechny členské státy EU. Ty si nemohou upravit pravidla odlišně. Proto je třeba zákon o ochraně osobních údajů upravit tak, aby byl v souladu s GDPR.

3.1 Hlavní znaky GDPR

Charakterizovat GDPR není pro mnohé zrovna jednoduché, je to nařízení, které nabylo platnosti a čeká na svou účinnost. Za hlavní znaky lze označit:

- je jednotně aplikovatelný na všechny země Evropské unie, bez rozdílů,
- rozšiřuje pojem osobních údajů, nově pracuje s pojmy jako biometrické prvky, a to z důvodu pokroku ve světě
- informace o zákazu používání předvyplněných políček, dochází tedy k zpřesňování souhlasu se zpracováním osobních údajů,
- vyšší technická a organizační bezpečnost správců a zpracovatelů, bude tedy nutné investovat větší náklady do ochranných prostředků.
- posílení práva fyzických osob a zakládání práv nových, a to například právo být zapomenut či právo na přenositelnost údajů.
- porušení ochrany nově musí být oznámeno a to nejpozději do 72 hodin, fyzické osobě, které se porušení týká, ale také Úřadu pro ochranu osobních údajů.
- vyšší sankce za porušení ochrany osobních údajů. Zde je podstatné zvýšení pokuty pro společnosti, které nesplňují nové nařízení. Sankce mohou být vybírány ve výšce větší než deset milionů eur nebo dvou procent celosvětového hrubého obrátu při porušení záznamů, bezpečnosti, porušení oznamování a posouzení dopadů na soukromí⁷⁰.

3.2 Základní povinnosti spojené s GDPR

Základní povinnosti, které s účinností nařízení GDPR nastávají, jsou převážně povinnosti o vedení záznamů o činnostech zpracování a posouzení vlivu na ochranu osobních údajů. Dále bude povinná konzultace s Úřadem pro ochranu osobních údajů, povinnost ohlašovat případy porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů a oznamování případů porušení zabezpečení osobních údajů subjektu údajů. Povinnost

⁷⁰ YELLAND, Bob. „How it Works“ GDPR. 2017. IBM Corporation.

jmenovat pověřence pro ochranu osobních údajů nebo takovou osobu zajistit externě. To vše a ještě mnohem více přichází s nařízením Evropské unie.

3.3 GDPR a zákon o ochraně osobních údajů

Nařízení Evropské unie o ochraně osobních údajů, nelze považovat za úplnou novinku. Faktem je, že toto nařízení pouze zpřisňuje a upřesňuje již existující pojmy. Pečlivěji charakterizuje pojmy, které jsou již známé. V následující Tabulce 1 jsou charakterizovány hlavní rozdíly GDPR a zákona o ochraně osobních údajů.

ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ	GDPR
Osobní údaje - jakákoliv informace týkající se určeného nebo určitelné fyzické osoby. Fyzická osoba se považuje za určenou nebo určitelnou, jestliže ji lze přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.	Osobní údaje - veškeré informace o identifikované nebo identifikovatelné fyzické osobě; identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.
Citlivý údaj - osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuální životě fyzické osoby a genetický údaj fyzické osoby; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci fyzické osoby.	Citlivé údaje - jsou speciální kategorií, která zahrnuje údaje o rasovém či etnickém původu, politických názorech, náboženském nebo filozofickém vyznání, členství v odborech, o zdravotním stavu, sexuální orientaci a trestních deliktech či pravomocném odsouzení osob. Nově zahrnuje genetické, biometrické údaje a osobní údaje dětí.
Anonymní údaj - takový údaj, který buď v původním tvaru, nebo po provedeném zpracování nelze vztáhnout k určené nebo určitelné fyzické osobě.	GDPR se nevztahuje na anonymní data.
Oznamovací povinnost – ten, kdo hodlá jako správce zpracovávat osobní údaje nebo změnit registrované zpracování je povinen tuto skutečnost písemně oznámit Úřadu pro ochranu osobních údajů před zpracováním osobních údajů.	Tato povinnost bude zrušena.
Likvidace osobních údajů – správce nebo na základě jeho pokynu zpracovatel je povinen provést likvidaci osobních údajů, jakmile pomine účel, pro který byly osobní údaje zpracovány, nebo na základě žádosti fyzické osoby	Právo být zapomenut – subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se dané fyzické osoby týkají, a správce má povinnost osobní údaje bez zbytečného odkladu vymazat.
Přístup subjektu údajů k informacím – požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.	Právo na přístup – fyzická osoba má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům.

Ochrana práv subjektů údajů – je-li žádost fyzické osoby shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závažný stav.	Právo na opravu – fyzická osoba má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje, které se jí týkají. S přihlédnutím k účelům zpracování má fyzická osoba práva na doplnění neúplných osobních údajů, a to i poskytnutím dodatečného prohlášení.
Toto právo není v zákoně upraveno.	Právo na přenositelnost údajů – fyzická osoba má právo získat osobní údaje, které se jí týkají, jež poskytla správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil.
Tato povinnost není v zákoně upravena.	Posuzování vlivu na ochranu osobních údajů – pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek vysoké riziko pro právo a svobody fyzických osob, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.
Tato povinnost není v zákoně upravena.	Pověřenec pro ochranu osobních údajů – správce a zpracovatel jmenují pověřence pro ochranu osobních údajů.
Tento časový údaj není v zákoně uveden.	Porušení ochrany dat – jakékoliv porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu.
Sankce – max. do výše 10 000 000 Kč (nebyla nikdy uložena).	Sankce – 10 000 000 EUR nebo do výše 2 % celkového ročního obrátu celosvětově za předchozí finanční rok, 20 000 000 EUR nebo do výše 4 % celkového ročního obrátu celosvětově za předchozí rozpočtový rok.

Tabulka 1: Rozdíly mezi zákonem a GDPR. (Zdroj: Hospodářská komora České republiky)

3.4 Základní povinnosti podnikatelů při ochraně osobních údajů

Zákon o ochraně osobních údajů ukládá podnikatelům základní povinnosti jak postupovat s osobními údaji. Tyto operace lze rozčlenit na osm základních skupin, které by podnikatel měl dodržovat. Jedná se především o:

- shromažďování osobních údajů,
- zpracování osobních údajů,
- uchovávání osobních údajů
- blokování osobních údajů,

- likvidace osobních údajů,
- zveřejňování osobních údajů,
- zpřístupnění osobních údajů,
- anonymizace osobních údajů.

3.4.1 Shromažďování osobních údajů

Za shromažďování lze označit systematický postup, jehož cílem je získání osobních údajů za účelem dalšího uložení na určený nosič, přičemž se počítá s dalším zpracováním těchto údajů. Toto usnesení je zakotveno v § 4 odstavce f) zákona č. 101/2000 Sb., o ochraně osobních údajů.

3.4.2 Zpracování osobních údajů

Při zpracování osobních údajů dochází k několika krokům, které jsou soustavou operací, které na sebe navazují. Jedná se o postup, který provádějí správci nebo zpracovatelé při své činnosti. Za zpracování lze označit výběr těchto dat, následné třídění a shromažďování daných dat, ukládání na dané nosiče a uchovávání. Dále zde lze uvést i zpřístupňování informací, úpravu či pozměňování daných údajů, vyhledávání, třídění nebo kombinování, blokování a následnou likvidaci.

3.4.3 Uchovávání osobních údajů

Za uchováváním osobních údajů vidíme takový proces, při kterém daný subjekt tyto informace uchová buď na vybraném nosiči, nebo v papírově podobě někde v databázi či archívu.

3.4.4 Blokování osobních údajů

Při blokování osobního údaje dochází k takovému stavu, že tento údaj je po určité době nepřístupný a nelze jej nijak zpracovávat či měnit. Samozřejmě nepřístupný musí být pro kohokoliv, nikoli tedy jen pro správce. Tento přístup je na rozdíl od likvidace pouze dočasný.

3.4.5 Likvidace osobních údajů

Likvidaci osobních údajů upravuje § 20 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve kterém je správce povinen provést likvidaci osobních údajů na základě žádosti subjektů nebo jakmile účel, pro který byly osobní údaje zpracovány, byl ukončen.

Zvláštní zákon stanoví výjimky týkající se uchovávání osobních údajů pro účely archivnictví a uplatňování práv v občanském soudním řízení, trestním řízení a správním řízení.

3.4.6 Zveřejňování osobních údajů

Zveřejňování osobních údajů je dnes nejvíce diskutované téma u jakékoliv společnosti. Jedná se o zpřístupnění sdělovacími prostředky nebo jiným veřejně známým sdělením. Toto sdělení je známo pouze neurčené skupině příjemců. V rámci této skutečnosti se jedná především o zveřejňování osob například v rejstříku dlužníků a podobně.

3.4.7 Zpřístupnění osobních údajů

Při zpřístupnění osobních údajů dochází k odhalení určitých části informací o daném subjektu. Zda se jedná o dotyčnou osobu, pozná jen okruh osob, kteří s touto osobou přišli do kontaktu. Tento přístup se využívá především u policie, kdy orgán veřejné moci zveřejní určitý počet informací, aby mohl nalézt hledanou osobu.

3.4.8 Anonymizace osobních údajů

Anonymizovaná data jsou taková data, která nepřímo nepomáhají identifikaci určité osoby a nejsou s nimi nijak propojená. Tyto anonymizovaná data jsou pro praktické využití vhodnější. Lze s nimi lépe nakládat a nejsou přímo regulovány přísnými pravidly o ochraně osobních údajů. Anonymizace osobních údajů lze provést několika technikami. Buď vyloučením základních identifikačních informací, nebo potlačením hodnoty. Další techniku, kterou lze využít při anonymizaci osobních údajů je zobecnění a seskupení.⁷¹

⁷¹ zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz*

PRAKTICKÁ ČÁST

4 Ochrana osobních údajů u vybraného podnikatele

Pro diplomovou práci byla vybrána společnost, která podniká na základě živnostenského oprávnění. Analýza byla prováděna v této společnosti na základě souhlasu majitele. Zkoumaná společnost se zabývá prodejem. Pro účely diplomové práce byl skutečný název společnosti změněn na společnost XY, z důvodu přání majitele nezveřejňovat název společnosti.

Společnost XY vznikl dne 14. června 2016 na základě zápisu u Krajského soudu v Ostravě.

4.1 Základní údaje společnosti

Datum vzniku	14. června 2016
IČO	051*****
Právní forma	Společnost s ručeným omezením
Předmět podnikání	Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona
Základní kapitál	50 000,- Kč
Vklad	50 000,- Kč
Splaceno	100%

Společnost má pro svůj prodej a prezentaci vytvořeny internetové stránky, které jsou nejdůležitějším článkem společnosti. Vzhledem k tomu, že je to pouze internetový obchod, a společnost nemá kamennou prodejnu, jsou dobře vytvořené internetové stránky základní povinností. Majitel proto vkládá nemalé finanční prostředky právě do správně zvoleného webového portálu, který má svou určitou doménu a na internetových vyhledávačích je dohledatelný.

Společnost se zabývá internetovým prodejem her do počítačů a dále online her, které jsou na dnešním trhu dostupné. V dnešní době mladých generací, které tráví na internetu dostatečný počet chvil, a kupují si mnohdy hry za kapesné od rodičů, je tento byznys velice

populární a takovýchto webových portálů existuje na internetu nespočet. Jinými slovy konkurence na tomto trhu je velická.

4.2 Zpracování osobních údajů společnosti XY

Majitel společnosti XY má zákonem stanovenou povinnost chránit osobní údaje. Od této povinnosti se žádný podnikatel nemůže oprostit. Podnikatel musí zpracovávat osobní údaje v souladu s pracovním zákoníkem, dále v souladu s novým občanským zákoníkem, zákonem o zaměstnanosti, a se zákonem o ochraně osobních údajů. V neposlední řadě lze také použít za pramen zákon o evidenci obyvatel a rodných číslech a zákon o archivnictví a spisové službě nebo důležitý zákon pro každého podnikatele, který má zaměstnance, a to o pojistném na sociálním zabezpečení a příspěvku na státní politiku zaměstnanosti a mnohá další.

Tyto zákony představují určitý právní rámec, který je závazný pro všechny podnikatele, bez rozdílu velikosti, základního kapitálu či oboru podnikání.

Majitel společnosti XY uchovává osobní údaje pomocí tištěné formy a také pomocí informačního systému. Pokud by u elektronického systému došlo k selhání, jsou tyto informace uchovány alespoň v tištěné a papírové podobě.

Tištěné dokumenty uchovává společnost v šanonech, každý ve složce v sídle podnikatele. Tyto šanony jsou přístupné pouze vedoucím pracovníkům a majitelům podniku, popřípadě následné kontrole, která by mohla přijít.

4.2.1 Zpracování osobních údajů před vznikem pracovního poměru.

V zákonu o ochraně osobních údajů § 4 písm. N) je definován souhlas subjektu se zpracováním osobních údajů takto: „*Svobodný a vědomý projev vůle subjektu údajů, jehož obsahem je svolení subjektu údaje zpracováním osobních údajů*“. Jednou ze základních zásad, na nichž GDPR stojí, je princip odpovědnosti správce osobních údajů. Uvedenou zásadu reflektují ustanovení článků 24 a 25 nařízení. Na základě těchto ustanovení musí příslušný správce splňovat veškeré povinnosti z nařízení plynoucí. Podnikatel, který zpracovává osobní údaje a je jejich správcem, má povinnost zavést vhodná technická a organizační opatření, aby byl schopen zajistit a doložit zpracovávání osobních údajů v souladu s GDPR⁷²

⁷² BARTÍK, V. a JANEČKOVÁ E.. *Ochrana osobních údajů v aplikační praxi. (vybrané problémy)*. Praha: Linde, 2009. ISBN 978-80-7201-740-9.

Zaměstnavatel společnosti XY si dobře uvědomuje skutečnost, že ochrana osobních údajů, nevzniká pouze při pracovně právním poměru, ale také před jeho samotným vznikem. Pokud přijímá zaměstnavatel nového pracovníka, je nutné vytvořit určitou nabídku práce a tu prezentovat na webovém portálu nebo oslovit úřad práce. V případě, že zvolí volbu inzerátu pomocí internetového portálu nebo v tištěné formě, je potřeba počítat s tím, že potenciální uchazeči na daný inzerát budou reagovat a posílat své životopisy s úvodními informacemi. Tímto krokem potenciální uchazeč souhlasí se zpracováním osobních údajů pro potřebu výběrového řízení. V první fázi zaměstnavatel XY tyto životopisy prochází a z nich vybírá do užšího výběru jen ty osoby, které podle vybraných kritérií nejlépe odpovídají pro zvolenou pozici. Po ukončení výběrového řízení a následném výběru vhodného kandidáta, zaměstnavatel uchovává životopisy ve speciální složce, která nese název životopisy.

Zaměstnavatel XY může požadovat informace, které nejsou v zákoně výslovně zakázány. Jsou to například informace jako jméno, příjmení, datum narození, město, odkud dojíždí a popřípadě kontakt, na který je možno jej informovat zda prošel do užšího výběru. Další informace, které může zaměstnavatel požadovat, jsou informace o dosaženém vzdělání a následné pracovní zkušenosti, popřípadě určité dovednosti a speciální dovednosti, které uchazeč získal během svého vzdělávání nebo z předchozího zaměstnání.

Další informace, které zaměstnavatel může požadovat v případě, že je pro to dán věcný důvod, který je důležitý pro práci, která má být vykonávána, představují dotčené informace. Ty představují převážně informace o trestně právní bezúhonnosti, majetkových poměrech, rodinných poměrech a popřípadě informace o těhotenství. Těhotenství je dost podstatným faktem, neboť v České republice existuje mnoho pracovních procesů, které by těhotné ženy ohrožovaly, případně by nebyly vhodné.

Další okruh představují informace, které zaměstnavatel nemůže nikdy po uchazeči požadovat a to jsou informace týkající se sexuální orientace, původu, členství v odborové organizaci, členství v politických stranách nebo příslušnost k určitému náboženství. Dotazování na podobné informace zakazuje zákon číslo 198/2009 Sb., o rovném zacházení a o právních prostředcích ochrany před diskriminací.

4.2.2 Zpracování osobních údajů v průběhu pracovního poměru

Druhou fází je zpracování osobních údajů zaměstnanců v průběhu pracovního poměru. V této fázi zaměstnavatel společnosti XY rozděluje shromažďování informací do dvou hlavních kategorií. Jedná se o informace, které jsou stanoveny přímo zákonem nebo to jsou

osobní údaje zaměstnanců, které nejsou definovány v zákoně. V první kategorii se jedná o informace, z oblasti sociálního zabezpečení a z oblasti daní. Zde musí zaměstnavatel vést evidenci docházky, neboli pracovní doby, pro výpočet mzdy a odvodu daně.

Druhou kategorií informací získává zaměstnavatel od zaměstnanců na základě vlastního uvážení. Další možnou skupinou jsou informace, které zaměstnavatel nemá povinnost shromažďovat, ale uzná-li to za vhodné, tak může tyto informace zpracovat.

Zaměstnavatel společnosti XY vede u každého svého zaměstnance osobní spis, ve kterém lze nalézt všechny nezbytné informace pro pracovní právní vztah daného zaměstnance. V osobním spise lze nalézt pracovní smlouvu, potvrzení o zdravotní způsobilosti, osobní dotazník, mzdový výměr, listiny prokazující účast zaměstnance na různých školeních a v neposlední řadě také souhlas se zpracováním osobních údajů. Co se týče osobního spisu, tak do něj mohou nahlížet jen vedoucí pracovníci, kteří jsou dotyčným zaměstnancem nadřazení. V tomto případě je to pouze zaměstnavatel. Mezi další subjekty, které mohou do spisu nahlížet, jsou státní orgány, které konají své povinnosti a provádí kontrolu. A poslední osobou, která do daného spisu může nahlížet, je sám zaměstnanec.

Údaje o mzdě jsou povinným údajem každé pracovní smlouvy. Ačkoliv tento údaj není v zákoně definován jako citlivý údaj, jsou zaměstnanci povinni o tomto údaji dodržovat mlčenlivost a zabezpečit tuto informaci proti jakémukoli zveřejnění.

4.2.3 Zpracování osobních údajů po skončení pracovního poměru

Zaměstnavatel společnosti XY po skončení pracovního poměru uchovává potřebné informace o zaměstnanci pro možné plnění v oblasti sociálního zabezpečení v daňové oblasti. Zaměstnavatel je potom povinen některé informace archivovat i po dobu několika let.

Při ukončení pracovního poměru zaměstnavatel vydává potvrzení o zaměstnání, ve kterém jsou jasně stanoveny údaje zákoníkem práce. S tím souvisí i pracovní posudek. Zaměstnavatel je povinen tento posudek vydat do 15 dní od žádosti zaměstnance. V dokumentu jsou uvedeny informace týkající se hodnocené práce, kvalifikace, schopností a dovedností, které se týkají vykonávané práce.

Doba uchování osobních údajů o zaměstnancích by měla být vázána na účel a důvody zpracování příslušných osobních údajů. Proto platí, že osobní údaje o zaměstnancích lze uchovávat tak dlouho, dokud trvá účel (účely) a zákonné důvody pro jejich zpracování. Není možné (ani vhodné) vyjmenovat taxativně uzavřený výčet údajů, které zaměstnavatelé o svých zaměstnancích z jednotlivých důvodů zpracování mohou zpracovávat. Zaměstnavatel

např. může (a na základě speciálních právních předpisů dokonce musí) z důvodu splnění své právní povinnosti uchovávat např. stejnopisy evidenčních listů po dobu 3 let, nebo mzdové listy nebo účetní záznamy o údajích potřebných pro účely důchodového pojištění po dobu 30 let,...“*údaje o druhu, vzniku a skončení pracovněprávního vztahu, záznamy o pracovních úrazech a o nemocech z povolání a záznamy o evidenci pracovní doby včetně doby pracovního volna bez náhrady příjmu.*“⁷³ Proto zaměstnavatel i po skončení pracovněprávního vztahu s příslušným zaměstnancem musí vyhodnotit, které údaje bývalého zaměstnance má evidovat a po jakou dobu. Jejich evidenci pak musí vést pro splnění právních povinností uložených mu speciálními právními předpisy.

4.3 Personální informační systémy

Jak již bylo zmíněno výše, osobní údaje jsou ve společnosti zpracovávány pomocí technologií a to pomocí počítačů nebo notebooků. Počítačové technologie usnadňují přístup běžným uživatelům. Nejen, že ji zrychlují, ale také zkvalitňují. Snižují personální náklady a zlepšují přehlednost daných údajů.

Masivní rozšíření nových technologií na pracoviště způsobilo radikální změnu v množství dat shromažďovaných o zaměstnancích a umožnilo jejich hromadění s dosud nevídanou systematičností a potenciální možností zásahu do práv zaměstnanců. Veliká část zaměstnanců používá k výkonu práce firemní počítač/notebook, chytrý telefon (a další chytrá zařízení), automobily a další zařízení a prostředky, které umožňují monitorování chování zaměstnanců. Navíc se výrazně stírá rozdíl mezi prací a soukromím. Zaměstnancům je často umožněno pracovat z domu s využitím technických prostředků poskytnutým zaměstnavatelem či se vzdáleným přístupem k zaměstnavatellovu software, kdy zaměstnanci mohou prostředky poskytnuté zaměstnavatelem využívat nejen k provádění pracovních úkolů, ale i pro volnočasové aktivity. Zaměstnavatel by proto měl nastolit rovnováhu mezi svým oprávněným zájmem před ztrátou svého majetku a know-how svěřeného zaměstnancům a mezi právem a oprávněným zájmem zaměstnanců na takovou kontrolu, která je přiměřená a nezasahuje v neodůvodněně vysoké míře do jejich soukromí.

⁷³ ŠKUBAL, Jaroslav, VEJSADA, Daniel. Doba uchování pracovněprávních dokumentů [online]. epravo.cz, 21. 1. 2013 [citováno 12. dubna 2018]. Dostupné na <<https://www.epravo.cz/top/clanky/doba-uchovanipracovnepravnich-dokumentu-88494.html>>.

4.4 COOKIES

Tak jako mnoho internetových stránek, tak i nejmenovaný webový portál využívá možnosti nových technologií, a tím jsou právě cookies. Do českého překladu můžeme toto slovo přeložit jako sušenky, s těmi fyzickými se ale nedají srovnávat. Jako cookies se v protokolu HTTP označuje malé množství dat, která www server pošle prohlížeči, který je uloží na počítači uživatele. Při každé další návštěvě téhož serveru pak prohlížeč tato data posílá zpět serveru. Cookies běžně slouží k rozlišování jednotlivých uživatelů, ukládají se do nich uživatelské předvolby apod. Může se jednat o data jako jméno, příjmení, emailová adresa uživatele, adresa domů nebo do zaměstnání, případně telefonní číslo, které zákazník na daném internetovém portálu vyplňuje. To znamená, že v případě, že vyplňujeme informace např. o doručení balíčku, který si na webovém portálu zakupujeme, musíme mít na paměti, a také být informováni o tom, že tato webová stránka využívá cookies. Při vyplňování identifikačních informací je povinnost majitele webového serveru upozornit zákazníka na to, že souhlasí se zpracováním osobních údajů.

Webové stránky jsou nastaveny tak, že jakmile se zákazník přihlásí na doménu s produkty daného podnikatele, otevře se oznamovací okénko, že tyto stránky využívají technologie cookies a zákazník musí následně potvrdit, zda se zpracováním osobních údajů souhlasí či nikoliv. V případě, že zákazník zaškrtně informaci, že je srozuměn s tím, že internetová stránka stahuje informace o uživateli, může si dané webové stránky prohlížet dál. Druhou variantou je, že zákazník nepotvrdí cookies a tak zakáže stahování informací o uživateli. Nevýhodou tohoto kroku je, že se stránky mohou zablokovat a tak si potenciální zákazník nezakoupí žádné zboží, neboť již se stránkou nemůže pracovat.

4.4.1 Lze cookies považovat za osobní údaje?

V dnešní uspěchané době se lze setkat z mnoho názory na cookies a lze se také dočíst informace, že cookies nejsou považovány za osobní údaje, nicméně jaká je vlastně skutečnost? Cookies neznamenají žádné nebezpečí pro počítač jako takový. Přesto cookies mohou být nebezpečné pro ochranu soukromí. Navštívený web si totiž může ukládat do cookies jakékoliv informace, které o návštěvníkovi zjistí a může tak postupně zjišťovat zájmy konkrétního návštěvníka - které stránky navštěvuje, jaké informace vyhledává, jak často daný web navštěvuje apod.

Těchto informací se dá posléze i bez vědomí návštěvníka využívat pro cílenou reklamu, statistické vyhodnocování chování návštěvníků, apod.

Tyto informace však lze získávat i bez cookies, proto toto jejich využití nemůže být považováno za zvlášť nebezpečné. Cookies lze zneužít zejména tehdy, pokud získá útočník přístup k počítači uživatele, neboť cookies na počítači nejsou nijak chráněny. Pak lze předstírat např. cizí identitu.

V rámci své působnosti si majitel společnosti XY dává pozor na to, aby všichni uživatelé odsouhlasili, že berou na vědomí, že vybrané stránky pracují s cookies a svým podpisem s tímto souhlasí. Každý takovýto souhlas s cookies musí odpovídat stanoveným pravidlům. Musí být učiněn svobodně, vědomě a jednoznačně, subjekt údajů může tento platný souhlas učinit i konkludentně⁷⁴. Majitel společnosti také upozorňuje své zákazníky o tom, že splňuje informační povinnost zveřejnit informaci, jakým způsobem budou dané informace zpracovány.

4.5 Příčiny zneužívání osobních údajů

Osobní údaje jsou v dnešní době velice podstatným pojmem. Každý den se na internetu pohybuje několik miliónů uživatelů, kteří zde hledají různé informace. Ale samozřejmě, že tam kde jsou informace, tam existují i lidé, kteří tyto informace chtějí zneužít. Jedná se o reklamní účely, krádeže identity na sociálních sítích nebo třeba také neoprávněné užívání dat ze strany policie a podobně. Zneužívání dat je velkým problémem, spolu s rostoucí oblibou sociálních sítí, kde lidé vkládají dobrovolně své údaje, nejen o své osobě, ale mnohdy také o svých blízkých a neuvědomují si, jaké jsou možné následky jejich jednání. Například Facebook. Problémy Facebooku vyplývají z koncentrace citlivých osobních dat a spousty aplikací, které k nim mají přístup. Aplikace může napsat kdokoli a poté data použít ke svým účelům. Facebook byl zakázán v některých pracovištích a školách pro sdílení nevhodného obsahu.

Samotné podmínky užití Facebooku velmi zasahují do práv a soukromí uživatelů, neboť obsahují oprávnění na použití veškerého obsahu podléhajícího duševnímu vlastnictví, který uživatel zveřejní na Facebooku nebo v návaznosti na něj, souhlas s přenesením a zpracováním osobních údajů uživatele, povolení použít jméno uživatele a profilové fotografie ve spojení s komerčním, sponzorovaným nebo souvisejícím obsahem a souhlas s případným odškodněním Facebooku za veškeré škody, ztráty a výdaje jakéhokoli druhu (včetně

⁷⁴ právní úkon učiněný jiným způsobem než ústně nebo písemně, ale takovým zřejmým jednáním vyjadřujícím jeho vůli jako účastníka právního úkonu (např. kývnutí hlavou, potřesení rukou, dodání zboží, nevyjádřením protestu)

přiměřených poplatků a nákladů na právní zastoupení) pokud vůči Facebooku vznesе žalobu související s kroky dotyčného uživatele.

Existuje ale také spousta jiných příkladů, kdy jsou zneužívány systémy. Například kamerové systémy na pracovišti jsou v případě špatné využitelnosti zaměstnavatele brány jako zneužívání osobních údajů.

4.6 Ochrana osobních údajů

Společnost XY se jako uvědomělá společnost snaží bránit osobní údaje co nejlépe a proto využívá hned několik možných řešení ochrany osobních údajů. Jedná se především o ochranu v rámci přístupových práv, dále pomocí kryptování, nebo využívá speciální router, který zabraňuje odcizení informací z daných portálů.

4.6.1 Přístupová práva

Zaměstnavatel společnosti XY řeší ochranu osobních údajů v rámci informačních systému pomocí ochrany přístupovými právy. Zaměstnanec, který se chce přihlásit do systému a pracovat v něm, musí použít své uživatelské jméno a příjmení, na který byl vytvořen uživatelský účet. Je nutné zadat následně své heslo, kterým je umožněn vstup do spravovaného informačního systému.

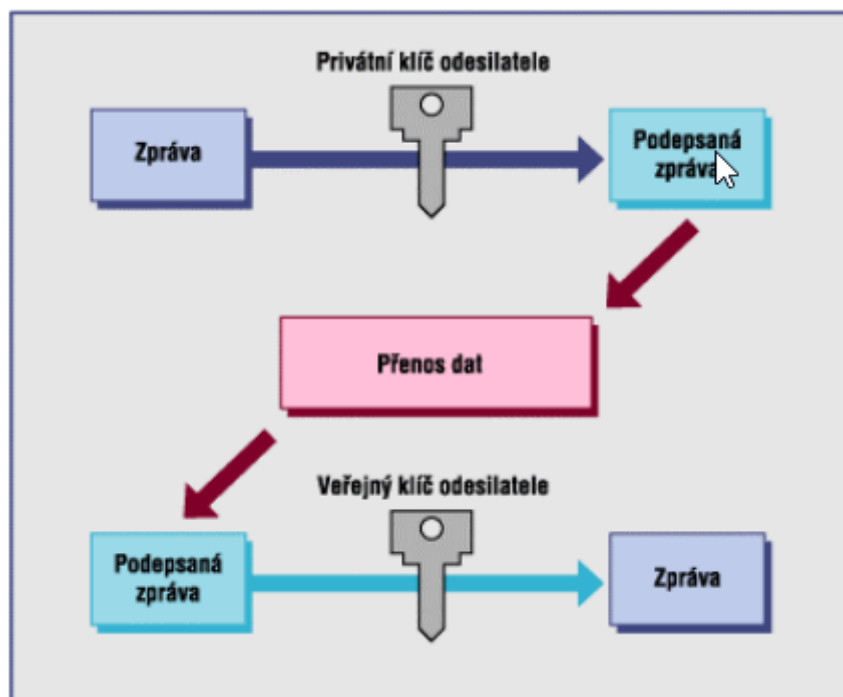
Společnost vůči svým zaměstnancům vytváří přístupová práva, která jsou chráněna proti případnému napadení jiným uživatelem. Každý zaměstnanec má své přihlašovací údaje a dále také své heslo, které si uschová a nesděljuje ho druhé straně.

4.6.2 Kryptování

V současné době je na světovém trhu několik desítek šifrovacích produktů, jež nabízejí různé funkce od pouhého off-line šifrování, přes kryptování obsahu disků nebo adresářů, až po on-line šifrování včetně plné integrace do operačního systému.

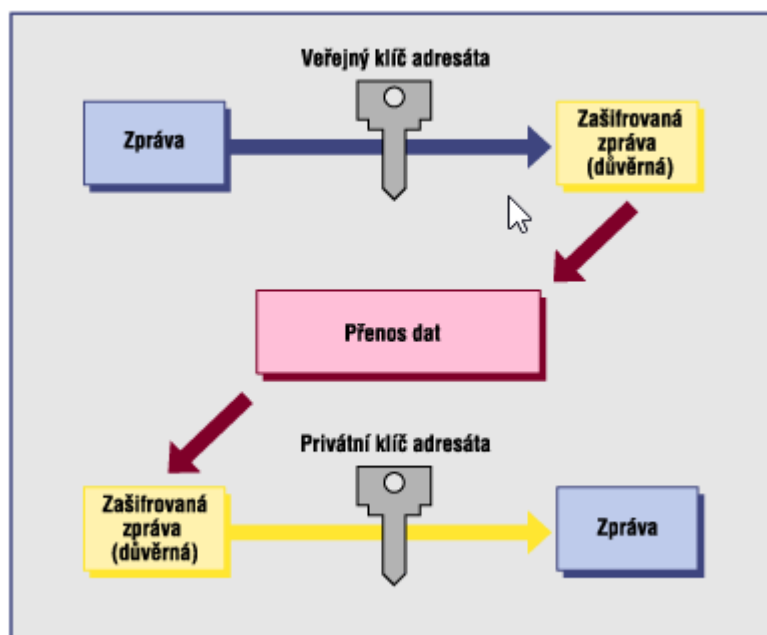
Do českého významu lze kryptování přeložit jako šifrování využívající přímo asymetrickou kryptografii. V systému se využívá jiný klíč pro šifrování, ale také jiný klíč pro dešifrování. Pro kryptování asymetrické se používá šifrovací klíč, který má dvě stránky, veřejný klíč a dešifrovací, neboli soukromý klíč. V případě, že uživatel navštíví daný portál a vygeneruje určitý produkt, stává se takzvaným majitelem obou klíčů. Princip je založen na faktu, že data jsou šifrovány jedním z klíčů, a ty lze dešifrovat pouze se znalostí druhého klíče a naopak. Jedná se o klasické pravidlo šifrování. Soukromý klíč je uchováván majitelem,

zatímco ten veřejný lze dohledat. Veřejný klíč je zveřejněn pro široký obsah uživatelů, a proto nemůžeme výše popsaný postup považovat za zcela zašifrovaný, lze jej chápat jako určitě popsaný.



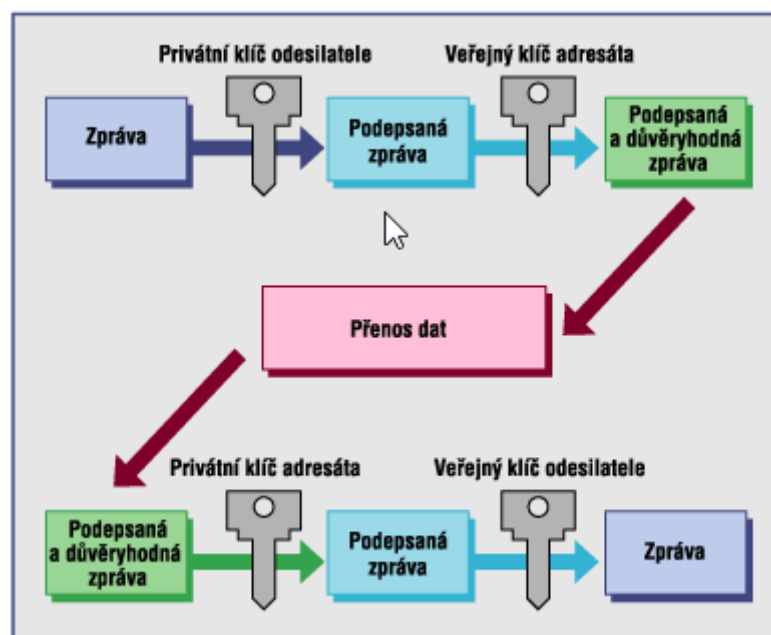
Obrázek 1: Přenos nezašifrované, ale podepsané zprávy. (Zdroj: http://mujweb.cz/tbu/asym_sifra.html)

Existuje ale také šifrování zpráv pomocí veřejného klíče adresáta. U této varianty existuje jistota, že tuto zprávu je schopen přečíst pouze adresát s privátním klíčem.



Obrázek 2: Přenos adresované, zašifrované, ale nepodepsané zprávy. (Zdroj: http://mujweb.cz/tbu/asym_sifra.html)

Celý systém šifrování a podepisování pracuje následujícím způsobem:



Obrázek 3: Přenos adresované, zašifrované a podepsané zprávy. (Zdroj: http://mujweb.cz/tbu/asym_sifra.html)

Existuje určitá zpráva na straně odesílatele, která je uživatelem podepsána a následně šifrována. Na straně druhé, straně příjemce, je zpráva dešifrována privátním klíčem příjemce. Zaručuje se tedy fakt, že zpráva je adresována a následně dochází za pomoci veřejného klíče k ověření identifikace odesílatele.

Na tyto skutečnosti existuje spousta algoritmů, které jsou velice využívány v informačních technologiích, a podstatu pro tyto šifrovací manévry tvoří matematické základy.

4.6.7 Router

Pro svou potřebu používá společnost speciální router, který zabráňuje kybernetickým útokům. Toto vybavení je nad rámec, ale majitel jej zakoupil pro zajištění ochrany soukromí. Při využívání tohoto routeru dochází ke zpracování osobních údajů ve velkém množství, a proto jsou tyto údaje monitorovány. Správcem údajů je společnost XY a ta určuje, jaký je účel využívání získaných kontaktů.

4.7 Archivace osobních dokumentů

Vzhledem k tomu, že je společnost na trhu teprve krátce a nemá historii, která sahá do desetiletí zpátky, a zaměstnanec má od prvopočátku podnikání. Ještě tudíž neměl možnost archivovat žádný osobní spis, který by mohl dát do archivačních desek. Nicméně ve své

kanceláři v sídle společnosti, má na tyto dokumenty určitý speciální přihrádku, kde se dokumenty, které podléhají archivaci, uchovávají.

Zákoník práce neukládá povinnost uchovávat dokumenty týkající se zaměstnanců jako pracovní smlouvy a podobně. Zákon o organizaci a provádění sociálního zabezpečení ale naopak nařizuje, že evidenční listy musí být uloženy po dobu tří let, záznamy o pojistném na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti se musí uchovávat šest let, mzdové listy a účetní záznamy pro účely důchodového pojištění, doklady o vzniku, druhu nebo skončení pracovněprávního poměru, záznamy o pracovních úrazech a nemocech z povolání, atd. musí být uchovávány třicet let.

4.8 Doporučení pro společnost

Po provedené analýze společnosti bylo zjištěno, že společnost dobře využívá technologie, které chrání osobní údaje. Má vhodně nastaveny i kvalitní bezpečnostní opatření, které potrápí jakéhokoliv narušitele. Přece jen bych společnosti XY doporučil určitá pravidla pro kvalitnější ochranu.

Například v rámci základních přístupových práv bych majiteli společnosti doporučil, aby vytvořil určitá kritéria, která by musel dodržet každý zaměstnanec. Heslo by mělo obsahovat kombinace velkých a malých písmen, dále by se v heslu měla objevovat kombinace čísel a speciálních znaků, které si uživatel zvolí sám.

Dalším vhodným postupem pro ochranu osobních hesel bych doporučil provádět pravidelná školení na téma, jak je důležité pro společnost heslo nikomu nezveřejňovat. Proškolení ohledně bezpečnostních pravidel není nikdy zbytečností.

Rady jsou následující:

- měnit heslo pravidelně,
- zabezpečit neopakování se hesel, v několika programech,
- heslo by mělo obsahovat malá i velká písmena, číslice a speciální znak,
- heslo by se mělo obnovovat, doporučuji třeba kvartálně,
- a nemožnost heslo opakovat.

Druhým doporučením v rámci informačního systému je využití jiné možnosti ochrany. Dnes existuje mnoho programů, které dokážou sledovat dané účty a s jistotou rozpoznají, zda se zaměstnanec připojil z jiného místa, než je obvyklé pro jeho pracovní zázemí. Výjimkou jsou služební cesty, kdy by daný program byl naprogramován tak, že by rozpoznal na základě zadaných informací, že je daný zaměstnanec služebně mimo.

S tím souvisí i fakt, že by společnost XY měla určit zodpovědnou osobu, která by měla ochranu osobních údajů na starost.

Hlavním doporučením je zaměřit se na nově platné, ale ještě neúčinné nařízení Evropské unie. Nejdůležitější kroky jsou shrnuty v následující kapitole 4.9 s názvem: Aplikace GDPR pro společnost XY. Zde jsou majiteli společnosti XY osvětleny důležité informace na co a jak se připravit, až vejde v účinnost nařízení GDPR.

4.9 Aplikace GDPR pro společnost XY

Společnost XY by se na GDPR měla připravit, neboť má pět zaměstnanců, okolo 5 000 zákazníků a provozuje e-shop, který je zaměřen na prodej her. Zaměstnavatel je zároveň správcem údajů. Vzhledem k tomu, že přichází v účinnost nové nařízení GDPR, je nezbytné pro společnost, aby se na nová pravidla připravila.

Vzhledem k tomu, že GDPR má lépe ochránit osobní údaje, je potřeba připravit pár kroků, které jsou nezbytné pro každou společnost. Každá společnost, každý podnik musí ochránit osobní údaje svých zaměstnanců, vzhledem k tomu, že GDPR bude postihovat celou společnost a ne jenom určité oddělení, které má osobní údaje na starosti. Je důležité, aby byl poučen i každý zaměstnanec.

Před zavedením GDPR je potřeba se zaměřit na interní audit. Vstupní audit by měl podnikateli primárně odpovědět na otázku, jaké osobní údaje zpracovává. Tento audit lze označit za první fázi před zavedením účinnosti nového nařízení. Audit by se měl zaměřit na aktuální zpracování osobních údajů ve společnosti XY. Dalším krokem je se zaměřit na jednotku, která osobní údaje zpracovává, ať už je to přímo majitel firmy, nebo například i externí firmy, které mohou mít tyto údaje na starost. Vzhledem k tomu, že společnost si zpracovává osobní údaje sama, nemusí se dále obracet na jiné externí firmy.

Dalším bodem této fáze je ověření místa uložení daných osobních údajů. Zda společnost využívá pro ukládání těchto údajů informační systémy nebo údaje uchovává pomocí šanonů a papírové formy.

Dalším krokem je zjištění na základě jakého titulu se osobní údaje zpracovávají. Společnost XY používá ke zpracování osobních údajů souhlas. Předposlední fází je pak uvědomění si účelu zpracovávání osobních údajů. Poslední fází je zjištění, na jak dlouhou dobu jsou osobní data zpracovávána. S tímto také souvisí archivace daných údajů.

Vzhledem k tomu, že GDPR je nejen velkou zodpovědností, ale také pro neznalé určitým strašákem, je potřeba, aby se do procesu implementace zapojil úplně každý. Je

potřeba vypracovat určitý harmonogram, s kterým bude zaměstnanec seznámen a bude do něj i zapojen.

Majitel společnosti by měl pověřit odpovědnou osobu, která připraví všechny potřebné náležitosti, zpracuje získané informace a vytvoří závěrečnou zprávu pro vedení společnosti. Tato osoba by měla mít dostatečné znalosti IT. Měla by dobře znát daná uložení a informace na nich uchovávané. V případě, že společnost využívá pro mzdové záležitosti externí osobu, měla by být vyrozuměna, že přijde v účinnost nová úprava zpracování osobních údajů a měla by dostat informaci, že daná společnost se změnou uchovávaní osobních údajů počítá, a že je na následné změny připravena formou navrhovaného řešení.

Po provedené analýze by měla společnost nastoupit na druhou fázi. Ta představuje úpravu vnitřních pravidel a norem procesů, které upravují ochranu osobních údajů. Měli by být například upraveny vnitřní dokumenty, mělo by dojít k zaškolení zaměstnanců, kteří nakládají s osobními údaji, připravit se na nové zpracování osobních údajů, zajistit zpracování záznamů o činnostech zpracování a nastavit určitá bezpečnostní pravidla.

GDPR neupravuje žádná povinnost pro osoby mít určité vzdělávání či vlastnit certifikaci, které tyto údaje zpracovávají. Jedinou podmínkou je, aby tato osoba měla praktické zkušenosti v oblasti ochrany osobních údajů a věděla, jak jsou v dané společnosti tyto údaje zpracovávány. Další důležitým okruhem je správné nastavení zabezpečení osobních údajů. Podle nařízení GDPR by osobní údaje měly být rozděleny na osobní a citlivé. V závislosti na obou kategoriích by měla být vypracována možná rizika, tzv. analýza rizik. Ta je charakterizována jako souhrnné vyhodnocení nebezpečí, které způsobí nebo může způsobit případnou škodu.

Společnost se také musí připravit na případné možné útoky na data, která uchovává. Nově v případě napadení a možného narušení má společnost povinnost vše oznámit do 72 hodin Úřadu pro ochranu osobních údajů. Také je potřeba tuto informaci oznámit i dotčené fyzické osobě. Posledním podstatným krokem, který je třeba zabezpečit, jsou technická opatření jako šifrování a chránění se proti odcizení údajů. Jde o bezpečnostní prvky, nikoli však o povinnost stanovenou zákonem nebo nařízením.

Třetí a poslední fází je následná realizace, implementace. Ta představuje nejdůležitější fázi v životě společnosti. Vzhledem k tomu, že při zpracování osobních údajů je největším rizikem jedinec, je potřeba, aby implementace byla provedena efektivně a prakticky. To spočívá především v pravidelném proškolení zaměstnanců a ověřování informovanosti svých podřízených. Následně je důležité ověřovat technickou úroveň daných informačních systémů, využívat neustálé aktualizace a používat různé ochranné prvky, které budou tyto

systémy chránit. V případě, že se podaří eliminovat rizika, je pravděpodobnost selhání při zavedení GDPR téměř nulová. Důležité je, aby informace o nastávající změně byly předávány všem zainteresovaným stranám, neboť připravenost na následující možnou změnu je důležitá.

Posledním krokem je bdění nad dodržováním nastavených změn a opatření, kdy bez jejich faktického vynucování by předchozí kroky vyšly vniveč.

4.9.1 Základní doporučení pro nadcházející účinnost GDPR:

- 1) Aktualizovat souhlasy se zpracováním osobních údajů podle GDPR.

V první řadě je důležité, aby se zákazníci dozvěděli o nadcházející změně v ochraně osobních údajů a dali k tomuto možnému kroku souhlas. Je třeba upravit dotaz při vyplňování osobních údajů a to tak, že je nově možné vložit předvyplněné zaškrtačací políčko. V případě, že společnost zvolí tuto možnost, je třeba informovat daného zákazníka, k jakému účelu jsou jeho osobní data využívána. Tato možnost se vztahuje pouze na nové zákazníky, kteří si pomocí webového portálu něco zakoupí. Varianta pro stávající zákazníky je následná: Pokud stávající zákazník již poskytl jednou souhlas se zpracováním osobních údajů, existuje velká pravděpodobnost, že tento souhlas poskytne znovu. Proto je možné řešení zaslání emailových zpráv těmto zákazníkům s následujícím obsahem:

Dobrý den pane/paní,

v květnu letošního roku vstoupí v účinnost nové **Nařízení Evropské unie o ochraně osobních údajů tzv. GDPR**, která nastavuje nová pravidla pro používání osobních údajů. Tomuto nařízení podléhají i Vaše data, která nám bylo poskytnuta během zakoupení našeho produktu na webových stránkách. Jedná se především o jméno, příjmení, adresu, kontaktní informace a podobně.

Rádi bychom si tyto informace i nadále ponechali, abychom Vás mohli v budoucnu kontaktovat případně určitých slevových akcí a zvýhodněných nabídek.

Proto Vás žádáme o svolení si Vaše osobní informace i nadále uchovávat. Postačí pouze svolení nadále tyto osobní informace spravovat. Jedná se o ty údaje, které již máme k dispozici. Pokud souhlasíte, prosím klikněte na níže uvedené tlačítko a potvrďte souhlas se zpracováním osobních údajů:

Souhlas se zpracováním osobních údajů

V případě, že se rozhodnete nám svoje svolení neposkytnout, stačí kliknout na „Odhlásit“ na konci tohoto emailu. Vymažeme Vaše osobní údaje a již Vás nebudeme moci oslovit s žádnou zajímavou nabídkou ve společnosti XY.

V případě jakýchkoliv dotazů mne neváhejte kontaktovat.

S přáním příjemného dne.

Podpis

Majitel XY

Základem úspěchu je pravidelná, jednoduchá komunikace. Zákazník musí být obeznámen s tím, kdo využívá jeho informace. Musí také vědět, k jakému účelu jsou tyto osobní informace zpracovávány, jak dlouho je daný subjekt bude uchovávat a v případě možného zpracování osobních údajů externí firmou musí zákazník vědět, kdo další bude s těmito údaji pracovat.

Velice důležitým faktem je, že v případě, že se na internetových portálech objeví informace o tom, že daný zákazník je mladší 16 let, je potřeba zákonná úprava a to souhlas rodičů nebo zákonného zástupce. Vzhledem k tomu, že na webových stránkách nakupují i děti, je potřeba se i na tuto informaci připravit.

2) Revidace smluv

Druhým bodem pro nadcházející účinnost GDPR je obnova smluvních vztahů. A to převážně na úrovni zaměstnavatele a zaměstnance. Smlouva musí nastavit povinnosti a odpovědnost za případnou škodu každé ze smluvních stran. V tomto případě je ujednání nezbytné, ale v případě, že by se jednalo o outsourcing⁷⁵, doporučuje se smluvní ujednání. Smlouva s externím dodavatelem zajišťuje, že jsou osobní údaje zpracovány v souladu se všemi obecně závaznými právními předpisy, neboť nově odpovědnost za řádné zpracování spadá i na zpracovatele.

⁷⁵ Outsourcing znamená, že firma vyčlení různé podpůrné a vedlejší činnosti a svěří je smluvně jiné společnosti

Závěrem je třeba si uvědomit, že neexistuje žádný expert, který by byl proškolen na zpracování osobních údajů podle GDPR. Toto nové nařízení nespadá pouze na jedince, ale na celou společnost a všechny zaměstnance. V případě, že ve společnosti neexistuje nikdo, kdo by porozuměl nové úpravě GDPR, je možnost obrátit se na externí poradce, kteří GDPR zpracovávají. Na trhu existuje mnoho společností, které nabízí případné řešení a zajištění souladu s GDPR. Tato skutečnost ovšem není v žádném zákoně nařízená a proto je důležité si rozmyslet, zda chce společnost do této možnosti investovat či nikoliv.

5 Závěr

Ochrana osobních údajů nemá komplexní zpracování, a proto při ochraně osobních údajů může jedinec sáhnout hned do několika úprav této problematiky. Po květnu se již bude moci zúčastněný jedinec obrátit také na nařízení GDPR, které tuto problematiku bude upravovat komplexněji. Neznamená to ovšem, že všechny platné zákony zde zanikají. Jedná se pouze o přijetí nového nařízení a tak se zákony stávají podpůrnými. To znamená, že to co není upraveno v nařízení, můžeme a musíme nalézt v zákoně.

Ochrana osobních údajů je velice specifickým tématem, neboť každá osoba má své osobní údaje, své práva a povinnosti a je potřeba se na tuto problematiku zaměřit. Každý podnikatel musí zabezpečit, že údaje, které získal pomocí svého podnikání, musí nějak uchovávat a ochraňovat.

Nařízení GDPR přináší v oblasti ochrany a zpracování osobních údajů několik úprav a novinek, na něž se musejí všechny organizace, co zpracovávají osobní údaje, včas připravit. Základním krokem pro přípravu na nové nařízení je podrobná analýza firemních procesů, při nichž dochází ke zpracování osobních údajů.

V teoretické části jsem se zaměřil na deskripci literatury, zařazen je zde rozbor všeobecných poznatků z oblasti ochrany osobních údajů. Je kladen důraz také na podrobnější vysvětlení pojmu osobní údaj. V praktické části práce byla provedena analýza procesů vybrané společnosti, na již základě byla definována specifika zpracování osobních údajů.

Diplomová práce, která byla zaměřena na vybranou společnost, měla být určitým návodem, jak s osobními údaji zacházet a pomocí analýzy by si čtenář, případně budoucí podnikatel měl uvědomit, že tuto záležitost nesmí nechávat na poslední chvíli.

Cílem práce bylo zhodnotit stávající systém ochrany soukromí a osobních údajů v dané společnosti. Dále čtenáře a majitele firmy seznámit s pojmem ochrana osobních údajů a pomoci jim udělat si pořádek v pojmech, které se týkají zpracování osobních údajů. Následně mu rozšířit informace, o tom, které možné zákony, směrnice, a nařízení tuto problematiku řeší. Obsah práce by měl být návodem pro ty, kteří nemají jistotu v tom, jaké jsou požadavky kladené podnikatelům GDPR a jak konkrétně tyto požadavky ve své společnosti zavést.

Přínos diplomové práce lze vidět ve vytvoření srozumitelného a strukturovaného přehledu dostupných informací o právní úpravě zpracování a ochrany osobních údajů v nařízení GDPR a představení návodů pro kontrolu aktuálních procesů a přípravu na vyhovění požadavkům stanoveným v nařízení GDPR. Informace zahrnuté v diplomové práci mohou

sloužit jako ucelený průvodce přípravami na soulad firemních procesů s nařízením GDPR nejen vedení vybrané společnosti, ale také jakékoliv jiné organizaci, která při své obchodní činnosti zpracovává osobní údaje.

Kapitoly 2 a 3 diplomové práce navíc mohou být pro jakoukoliv fyzickou osobu stručným a přehledným zdrojem základních informací o problematice zpracování a ochrany osobních údajů a právech subjektu osobních údajů, jež by měl každý člověk alespoň rámcově znát. Své osobní údaje je potřebné chránit proti zneužití či neoprávněnému zpracování a právě znalost práv subjektu osobních údajů a zvýšená obezřetnost při sdílení osobních údajů jsou základními principy, podle nichž může v každodenní praxi každá fyzická osoba kontrolovat, zda dochází ke zpracování jejích osobních údajů pouze v souladu s právními předpisy.

Seznam použité literatury

- BARTÍK, V. a JANEČKOVÁ E. *Ochrana osobních údajů v aplikační praxi. (vybrané problémy)*. Praha: Linde, 2009. ISBN 978-80-7201-740-9.
- BLACKMER, W.S. 2016. “GDPR: Getting Ready for the New EU General Data Protection Regulation”. Information Law Group. InfoLawGroup LLP.
- CEJPEK, Jiří. *Informace, komunikace a myšlení*. Praha : Univerzita Karlova v Praze. Nakladatelství Karolinum, 2005. 233 s.
- HENDRYCH, D. a kol. *Právníký slovník*. 2. rozšířené vydání. Praha: C. H. Beck, 2003, 983 s. ISBN 80-7179-740-5
- Charta Organizace spojených národů a Statut Mezinárodního soudního dvora*. Praha: Informační centrum OSN, 1998, ISBN 80-238-5263-9
- KUČEROVÁ, Alena a František NONNEMANN. *Ochrana osobních údajů v praktických příkladech*, Praha, Vydavatel : RNDr. Ivana Hexnerová – BOVA POLYGON, 2013, 78 s., ISBN 978-80-7273-173-2
- KUČEROVÁ, Alena. *Zákon o ochraně osobních údajů: komentář*. ISBN 978-807-1792-260.
- MAAYTOVÁ, A., F. OCHRANA a J. PAVEL. *Veřejné finance v teorii a praxi*. Praha: GradaPublishing, 2015. Expert (Grada). ISBN 978-80-247-5561-8.
- MAŠTALKA, Jiří. *Osobní údaje, právo a my*. 1. vydání. Praha: C. H. Beck, 2008, 33 s. ISBN 978- 80- 74-00-033-1
- MATES, Pavel. *Ochrana osobních údajů*. Vyd. 1. Praha: Karolinum, 2002, s. 37. ISBN 80-246-0469-8
- MATES, P., E. JANEČKOVÁ a V. BARTÍK: *Ochrana osobních údajů*. Praha: Leges, 2012, 19 s. ISBN 978-80-87576- 12- 0
- MATOUŠOVÁ, Miroslava a Ladislav HEJLÍK. *Osobní údaje a jejich ochrana. Knížka pro praxi*. 1. vydání. Praha : ASPI, 2003, 34 s.ISBN: 80-7357-322-9
- MORÁVEK, Jakub. *Ochrana osobních údajů v pracovněprávních vztazích*. Praha: Wolters Kluwer, 2013, s. 58. ISBN 978-80-7478-139-1
- PRŮCHA, Petr. *Základy správního práva a veřejné správy, obecná část*. 2. přepr. a dopl. vyd. Brno: MU v Brně, 1994. 260 s. ISBN 80-210-0886-5.

SMEJKAL, V. a kol. *Právo informačních a telekomunikačních systémů*. 2. vydání. Praha: C.H.Beck, 2004, 161 s.

TELEC, Ivo. *Chráněné statky osobnostní, Právní rozhledy*. 2007, roč. 15, s. 273. ISSN 1210-6410

YELLAND, Bob. „*How it Works*“ *GDPR*. 2017. IBM Corporation. 13 s.

Zákony a nařízení:

Zákon č. 89/2012 Sb. - Občanský zákoník

Ustanovení § 4 písm. k) ZOOÚ

Všeobecná deklarace lidských práv, New York, 10. prosince 1948, článek 12

Zákon o ochraně osobních údajů č. 101/2000 Sb.

Úmluva č. 108, čl. 5 – pís. a),b),c),d),e)

Úmluva č. 108, čl. 6

Úmluva č. 108, čl. 8

Internetové zdroje:

ČESKO. § 5 odst.1 zákona č. c),d),e),f) zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p5-1-c,d,e,f>

ČESKO. § 4 písm. j) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-j>

ČESKO. § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-a>

ČESKO. § 4 písm. b) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-b>

ČESKO. § 13 odst.1,2 zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p13-1,2>

ČESKO. § 3 odst. 3 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106#p3-3>

ČESKO. fragment #f1945949 zákona č. 106/1999 Sb., o svobodném přístupu k informacím. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/1999-106#f1945949>

ČESKO. § 4 písm. e) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. In: *Zákony pro lidi.cz* [online]. © AION CS 2010-2018 [cit. 16. 2. 2018]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2000-101#p4-1-e>

Hospodářská komora České republiky. Nová pravidla ochrany osobních údajů: Měníme vize ve skutečnost [online]. 2017, [cit. 2018-03-24]. Dostupné z: https://www.komora.cz/files/uploads/2017/06/2017_11_16P%C5%99%C3%ADru%C4%8Dka-GDPR_final2.pdf

KADLEČKA, Stanislav a Filip RIGEL. *Výkon státní správy – kompetence, odpovědnost* [online]. 16. září 2009, [cit. 2018-02-21]. Dostupné z: www.mvcr.cz/soubor/vykon-statni-spravy-kompetence-pdf.aspx

NOVÁ PRAVIDLA OCHRANY OSOBNÍCH ÚDAJŮ: Měníme vize ve skutečnost [online]. Vydala Hospodářská komora České republiky, Odbor legislativy, práva a analýz, 2017, květen 2017, [cit. 2018-02-16]. Dostupné z: <https://www.uoou.cz/zakladni-prirucka-k-gdpr/ds-4744/archiv=0&p1=4069>
https://www.uoou.cz/files/ldv_prirucka_cz.pdf

<https://www.uoou.cz/lze-souhlas-se-zpracovanim-osobnich-udaju-ve-smyslu-5-odst-4-zakona-o-ochrane-osobnich-udaju-ucinit-i-elektronickymi-prostredky-napr-pres-internet/d-11336>

<https://www.zakonyprolidi.cz/cs/1992-209>

<http://www.eurlex.cz/dokument.aspx?celex=31995L0046,čl. 1, čl. 3>

<https://www.psp.cz/docs/laws/listina.html>

<https://www.psp.cz/docs/laws/listina.html>

<https://www.zakonyprolidi.cz/cs/2000-101#cast1 § 3 odst 5>

<https://www.zakonyprolidi.cz/cs/2000-101#cast1 § 3 odst 3,4>

<http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32002L0058&from=CS, odstavec 46>

<http://www.oecd.org/sti/ieconomy/15589535.pdf>

<https://www.ibm.com/data-responsibility/gdpr/>

Prohlášení o využití výsledků diplomové práce

Prohlašuji, že

- jsem byl seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. – autorský zákon, zejména § 35 – užití díla v rámci občanských a náboženských obřadů, v rámci školních představení a užití díla školního a § 60 – školní dílo;

- beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB-TUO) má právo nevýdělečně, ke své vnitřní potřebě, diplomovou práci užít (§ 35 odst. 3);

- souhlasím s tím, že diplomová práce bude v elektronické podobě archivována v Ústřední knihovně VŠB-TUO a jeden výtisk bude uložen u vedoucího diplomové práce. Souhlasím s tím, že bibliografické údaje o diplomové práci budou zveřejněny v informačním systému VŠB-TUO;

- bylo sjednáno, že s VŠB-TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona;

- bylo sjednáno, že užít své dílo, diplomovou práci, nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB-TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB-TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 26.4.2018



Bc. Martin Václavík, DiS.

Seznam použitých zkratek

GDPR/Nariadenie	nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
Směrnice 94/95/ES	Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
ČR	Česká republika
EU	Evropská unie
DPO/Pověřenec	Data Protection Officer (pověřenec pro ochranu osobních údajů)
Podnikatel	podnikatelem se pro účely této práce myslí malý a střední podnikatel
Working Party 29	pracovní skupina zřízená jako poradní sbor dle článku 29 směrnice 94/95/ES
ÚOOÚ/Úřad	Úřad pro ochranu osobních údajů
SDEU	Soudní dvůr Evropské Unie
ESLP	Evropský soud pro lidská práva
Občanský zákoník	zákon č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů
Zákoník práce	zákon č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů.
Zákon o ochraně osobních údajů	zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů